S. Hrg. 99-299

THE NATIONAL SECURITY PROTECTION ACT OF 1985

HEARING

BEFORE THE

SUBCOMMITTEE ON
MANPOWER AND PERSONNEL

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

NINETY-NINTH CONGRESS

FIRST SESSION

ON

S. 1301

TO STRENGTHEN THE COUNTERINTELLIGENCE CAPABILITIES OF THE DEPARTMENT OF DEFENSE, TO AMEND THE UNIFORM CODE OF MILITARY JUSTICE TO ESTABLISH PENALTIES FOR ESPIONAGE IN PEACETIME, TO PROVIDE INCREASED PENALTIES FOR ESPIONAGE, AND FOR OTHER PURPOSES

JUNE 26, 1985

Printed for the use of the Committee on Armed Services

U.S. GOVERNMENT PRINTING OFFICE
54-169 O WASHINGTON : 1985

5201-3

COMMITTEE ON ARMED SERVICES

BARRY GOLDWATER, Arizona, *Chairman*

STROM THURMOND, South Carolina
JOHN W. WARNER, Virginia
GORDON J. HUMPHREY, New Hampshire
WILLIAM S. COHEN, Maine
DAN QUAYLE, Indiana
JOHN P. EAST, North Carolina
PETE WILSON, California
JEREMIAH DENTON, Alabama
PHIL GRAMM, Texas

SAM NUNN, Georgia
JOHN C. STENNIS, Mississippi
GARY HART, Colorado
J. JAMES EXON, Nebraska
CARL LEVIN, Michigan
EDWARD M. KENNEDY, Massachusetts
JEFF BINGAMAN, New Mexico
ALAN J. DIXON, Illinois
JOHN GLENN, Ohio

JAMES F. MCGOVERN, *Staff Director and Chief Counsel*
ARNOLD L. PUNARO, *Staff Director for the Minority*
ALAN R. YUSPEH, *General Counsel*
CHRISTINE C. DAUTH, *Chief Clerk*

SUBCOMMITTEE ON MANPOWER AND PERSONNEL

PETE WILSON, California, *Chairman*

STROM THURMOND, South Carolina
WILLIAM S. COHEN, Maine
JOHN P. EAST, North Carolina
JEREMIAH DENTON, Alabama

JOHN GLENN, Ohio
SAM NUNN, Georgia
J. JAMES EXON, Nebraska
EDWARD M. KENNEDY, Massachusetts

CONTENTS

CHRONOLOGICAL LIST OF WITNESSES

Page

Snider, L. Britt, Principal Director, Counterintelligence and Security Policy, Office of the Secretary of Defense, accompanied by Jack Donnelly, Director, Counterintelligence and Investigative Programs, and Mayrard Anderson, Director, Security Plans and Programs 12

Cox, Hon. Chapman B., general counsel, Department of Defense 41

S201-3

THE NATIONAL SECURITY PROTECTION ACT OF 1985

WEDNESDAY, JUNE 26, 1985

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON MANPOWER AND PERSONNEL,
Washington, DC.

The subcommittee met in open session, pursuant to notice, at 2:07 p.m., in room SR-232A, Russell Senate Office Building, Senator Pete Wilson (chairman) presiding.

Present: Senators Wilson, Cohen, Denton, Gramm, Nunn, Exon, Levin, Bingaman, and Glenn.

Staff present: Alan R. Yuspeh, general counsel; Arnold L. Punaro, staff director for the minority; Patrick A. Tucker, counsel; Jeffrey H. Smith, minority counsel; Patricia L. Watson, research assistant; Jonathan L. Etherton, George K. Johnson, Jr., and David S. Lyles, professional staff members; and Mary J. Kampo, staff assistant.

Also present: James H. Dykstra, assistant to Senator Cohen; Mark J. Albrecht, assistant to Senator Wilson; Allan W. Cameron, assistant to Senator Denton; Alan Ptak, assistant to Senator Gramm; Jeffrey B. Subko, assistant to Senator Exon; James B. Steinberg, assistant to Senator Kennedy; Edward McGaffigan, Jr., assistant to Senator Bingaman; and Phillip P. Upschulte, assistant to Senator Glenn.

[The bill S. 1301 follows:]

99TH CONGRESS
1ST SESSION

S. 1301

To strengthen the counterintelligence capabilities of the Department of Defense, to amend the Uniform Code of Military Justice to establish penalties for espionage in peacetime, to provide increased penalties for espionage, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 13 (legislative day, JUNE 3), 1985

Mr. GRAMM (for himself, Mr. GOLDWATER, Mr. THURMOND, Mr. DOLE, and Mr. HELMS) introduced the following bill; which was read twice and referred to the Committee on Armed Forces

---

A BILL

To strengthen the counterintelligence capabilities of the Department of Defense, to amend the Uniform Code of Military Justice to establish penalties for espionage in peacetime, to provide increased penalties for espionage, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

SECTION 1. This Act may be cited as the "National Security Protection Act of 1985".

CONGRESSIONAL FINDINGS AND POLICIES

SEC. 2. The Congress finds—

(1) that there have been recent cases of disclosures of classified information to the Soviet Union with serious consequences to the national security of the United States;

(2) that such treacherous actions reflect the most reprehensible conduct on the part of citizens of the United States and should be subjected to the most severe penalties;

(3) that an excessively large number of individuals who are members of the Armed Forces of the United States or civilian employees of the Department of Defense presently hold clearances granting them access to classified information, and that such excessive access to classified information increases the likelihood of unauthorized disclosure of such information to foreign governments; and

(4) that currently available means of technology have not been used to the fullest possible extent to uncover ongoing cases of espionage.

COUNTERINTELLIGENCE CAPABILITIES OF THE DEPARTMENT OF DEFENSE

SEC. 3. The Secretary of Defense shall submit a report to the Congress within 180 days after the date of the enactment of this Act on the existing capabilities of the military departments and the Office of the Secretary of Defense to conduct counterintelligence operations. The Secretary shall include in such report a description of any changes to existing capabilities which the Secretary proposes to implement in order to enhance counterintelligence operational capability in the Department of Defense. The Secretary shall also state in such report whether the Secretary regards the resources available to him for the purpose of conducting counterintelligence operations as adequate. In the event the Secretary determines that additional resources are necessary, he shall identify the type and amount of such additional resources required to meet counterintelligence requirements.

SECURITY CLEARANCES

SEC. 4. The Secretary of Defense shall submit a report to the Congress not later than 180 days after the date of the enactment of this Act on plans of the Secretary for a reduction in the number of members of the Armed Forces of the United States and civilian employees of the Department of Defense who hold clearances granting them access to classified information. The Secretary shall include in such report a schedule for the appropriate implementation of such a plan.

AMENDMENTS TO THE UNIFORM CODE OF MILITARY JUSTICE

SEC. 5. (a) Chapter 47 of title 10, United States Code, is amended by inserting after section 906 the following new section:

"§ 906a. Art. 106a. Espionage in time of peace

"Any person subject to this chapter who at any time, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be tried by a general court-martial and on conviction shall be punished by death or by imprisonment for any term of years or for life, except that if the foreign government is the Government of the Soviet Union or any other Communist country (as previously determined and publicly proclaimed by the President), such person shall upon conviction be punished by death or mandatory life imprisonment.".

(b) The table of sections at the beginning of subchapter X of such chapter is amended by inserting after the item relating to section 906 the following new item:

"906a. Art. 106a. Espionage in time of peace.".

POLYGRAPH EXAMINATIONS FOR COUNTERINTELLIGENCE

SEC. 6. (a) The Secretary of Defense shall require polygraph examinations to assist in determining the initial eligibility of persons to have access to sensitive compartmented information and shall aperiodically thereafter use such examinations to assist in determining the continued eligibility of such persons to have access to sensitive compartmented information.

(b) The Secretary of Defense may require polygraph examinations to assist in determining the initial eligibility of persons to have access to classified information other than sensitive compartmented information and may use such examinations aperiodically thereafter to assist in determining the continued eligibility of such persons to have access to such classified information.

(c) The results of polygraph examinations shall not be used as the sole basis for denying eligibility for clearance or access to any classified information.

(d) Individuals who refuse to submit to polygraph examinations conducted pursuant to the authority of this section may be denied clearance or access to classified information, or, if clearance or access has already been granted, may have their clearance or access withdrawn.

(e) The polygraph examinations authorized or required by this section shall be restricted to relevant issue questions which are intended to elicit an indication of whether a person has or plans to make unauthorized disclosure of classified information, or to take any other action which would violate the espionage laws of the United States.

(f) The Secretary of Defense shall report to the Congress not later than 180 days after the date of the enactment of this Act on plans developed by the Secretary to implement this section.

AMENDMENTS TO FEDERAL ESPIONAGE LAW

SEC. 7. Section 794 of title 18, United States Code, is amended by adding at the end thereof the following new subsection:

"(d) The death penalty for subsection (a) of this section may only be adjudged if the jury, or if there is no jury, the court, finds beyond a reasonable doubt, that the foreign government involved is the Soviet Union or any other Communist country (as previously determined and publicly proclaimed by the President) and that the document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information involved is classified.

"(e) The death penalty for subsection (b) of this section may only be adjudged if the jury, or if there is no jury, the court, finds beyond a reasonable doubt, that the foreign government involved is the Soviet Union, any other Communist country (as previously determined and publicly proclaimed by the President), or an enemy of the United States and that the document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information involved is classified.".

MANDATORY LIFE TERM OF IMPRISONMENT FOR SOVIET ESPIONAGE

SEC. 8. (a) Section 794(a) of title 18, United States Code, is amended by striking out the period at the end and inserting in lieu thereof the following: "; except that if the foreign government is the Government of the Soviet Union or of any other Communist country (as previously determined publicly and proclaimed by the President), any person convicted under this subsection shall be punished by death or be imprisoned for the rest of such person's life. Notwithstanding any other provision of law, the court, in imposing a life sentence under the exception in the preceding sentence, may not sentence the defendant to probation, nor suspend such sentence, and the defendant shall not be eligible for release on parole.".

(b) Section 794(b) of such title is amended by striking out "for any term of years or for life." and inserting in lieu thereof "for the rest of his life. Notwithstanding any other provision of law, the court, in imposing a life sentence under this subsection, may not sentence the defendant to probation, nor suspend such sentence, and the defendant shall not be eligible for release on parole.".

EFFECTIVE DATE

SEC. 9. The amendments made by this Act shall be applicable to offenses committed on or after the date of the enactment of this Act.

OPENING STATEMENT BY SENATOR PETE WILSON, CHAIRMAN

Senator WILSON. Good afternoon.

The Subcommittee on Manpower and Personnel will come to order.

The subcommittee meets today to conduct the first of a planned series of three hearings on S. 1301, the National Security Protection Act of 1985, introduced on June 13, 1985, by Senators Gramm, Goldwater, Thurmond, Dole, and Helms.

This legislation has been referred to the Armed Services Committee and subsequently to the Manpower and Personnel Subcommittee because of the committee's jurisdiction over proposed legislation and other matters relating to the common defense, to the Department of Defense and the military departments and to the programs regulating the conduct of members of the Armed Forces, specifically including the Uniform Code of Military Justice.

S. 1301 will address four related issues.

First, the bill would require reports from the Secretary of Defense on the capabilities of and resources available to the military departments and to the Department of Defense to conduct counterintelligence operations.

It would place on the Secretary of Defense the requirement to report on the Secretary's plans to reduce the number of military personnel and civilian employees of the Department of Defense who have clearance for access to classified information.

Second, the bill would require—I underscore require—the use of initial and periodic polygraph examinations of those persons seeking, or having clearance or access, to sensitive compartment information and would permit, not require, but permit, such polygraph examinations of persons seeking or having the clearance for access to all other levels of classified information.

Third, the bill would establish for the first time a capital offense under the Uniform Code of Military Justice that would proscribe espionage activities during the period other than wartime by persons subject to the Code of Military Justice.

If the offense involved the Soviet Union or any other Communist country proclaimed by the President, the only permissible sentences upon conviction would be life imprisonment or death.

Finally, the bill would amend section 794 of title 18 of the United States Code, one of several Federal criminal espionage statutes, to provide in the cases of espionage, involving the Soviet Union or any other Communist country in peacetime, that the only permissible sentences upon conviction would be death or life imprisonment without suspension, probation or parole.

I am aware of some questions being raised by the jurisdiction of the Armed Services Committee over the subject matter of S. 1301, at least with regard to that portion of the bill which would amend title 18 of the United States Code.

Let me say that there should be little doubt that the subject matter of S. 1301 is directly and clearly related to the common defense of this nation, a matter over which the Armed Services Committee has sole jurisdiction.

At the same time I clearly recognize and respect the jurisdiction of the Judiciary Committee and its distinguished chairman, my friend and colleague, Senator Thurmond, over matters involving civilian espionage.

Therefore, I fully intend to work closely with Senator Thurmond and the Judiciary Committee as this bill moves through the Senate.

Today we will hear from two witnesses from the Department of Defense who will give us an overview of the problems confronted by the Department relating to espionage and counterintelligence, and will provide the Department's comments and views on the bill before us.

First, we will hear from Mr. L. Britt Snider, Principal Director, Counterintelligence and Security Policy in the Office of the Secretary of Defense.

Then we will receive testimony from the Honorable Chapman B. Cox, General Counsel of the Department of Defense who will provide us some insight over the legal issues raised by espionage activities.

While they may be in the news and clearly have been on each of our minds, obviously we will avoid questioning these witnesses about ongoing criminal investigations of espionage offenses.

It would be inappropriate for senior officers in the executive branch to comment on facts or evidence with respect to cases presently before the Federal courts.

I welcome our witnesses and thank you for appearing today.

Before receiving testimony, I would have yielded to the distinguished ranking minority member, Senator Glenn, who will be with us presently, however he indicated his desire that we proceed without him.

We are expecting, in addition to regular members of the subcommittee, a number of members whose interest in this has caused them to attend.

We welcome Senator Bingaman and will invite him to take part. The distinguished Senator from Georgia, Senator Nunn, is also a member of the subcommittee.

It is the plan of the Chair, if we have the attendance that I am expecting, to use a system of alternating the questioning. We will, of course, invite nonmembers who care to participate to question the witnesses.

Let us begin by having 10-minute rounds and see how that goes.

Senator Nunn, do you have a statement you would care to make?

Senator NUNN. No, not now, Mr. Chairman. I am very interested in the subject. I am pleased you are holding this hearing. I think it is enormously important. I look forward to the testimony.

Senator WILSON. Senator Bingaman.

Senator BINGAMAN. I have no opening statement. I appreciate the chance to be here.

Senator WILSON. In that case, I will invite Senator Gramm, the sponsor of this legislation to tell us what he wishes to before we begin the testimony from the witnesses.

Senator GRAMM. Thank you, Mr. Chairman.

Mr. Chairman, you have outlined the bill. I would just like to thank you for holding the hearing.

I think what we are trying to do here is to deal with a problem that clearly is present today, but a problem that is going to become more serious as the new technology that we have developed in the last 5 years, with massive investment in R&D, begins to move from the scientific laboratories, where that technology is in the hands of a relatively few thousand people to prototype development production, where literally tens of thousands of people will at some point have access to that technology.

I think what we need here is a reasoned approach. The reason I wanted to introduce a bill that had four major parts that sought to deal with the entire problem is that we want some happy medium between a series of amendments that are offered with no hearings, with no logical consistency that we all vote for because we are concerned about the problems, versus the alternative which is no action at all.

So, the objective here was to sit down with the Defense Department, with the chairman of the Judiciary Committee, with the chairman of the Armed Services Committee, and especially in light of what we have learned from the *Walker* case, and try to put together a comprehensive bill to deal with the problem; instead of trying to attach that piece of legislation as a rider or an amendment to another bill, to have a series of hearings to debate the issue in full and then to move ahead, hopefully with Senate and House approval.

The objective is, therefore, to deal with the problem and I want to thank you for starting the ball rolling with this hearing.

Senator WILSON. Thank you, sir.

Let us proceed to receive the statement of L. Britt Snider, Principal Director of Counterintelligence and Security Policy in the Office of the Secretary of Defense.

STATEMENT OF L. BRITT SNIDER, PRINCIPAL DIRECTOR, COUNTERINTELLIGENCE AND SECURITY POLICY, OFFICE OF THE SECRETARY OF DEFENSE, ACCOMPANIED BY JACK DONNELLY, DIRECTOR, COUNTERINTELLIGENCE AND INVESTIGATIVE PROGRAMS, AND MAYNARD ANDERSON, DIRECTOR, SECURITY PLANS AND PROGRAMS

Mr. SNIDER. Thank you, Mr. Chairman.

With your permission, I would like to read most of my prepared statement and then I will be pleased to respond to any questions you may have.

Senator WILSON. Go ahead.

Mr. SNIDER. Mr. Chairman, it is a pleasure to appear before this subcommittee this afternoon.

I have been asked to describe the programs the Defense Department has ongoing to prevent and detect hostile intelligence activities undertaken against our employees and contractors, and to comment upon the provisions of S. 1301, now pending before the subcommittee.

Accompanying me are Mr. Jack Donnelly, who is Director for Counterintelligence and Investigation Programs, and Mr. Maynard Anderson, who is Director for Security Plans and Programs, both of our office.

By way of introduction, we all work for the Under Secretary of Defense for Policy within the Office of the Secretary of Defense, Dr. Ikle, who has overall policy responsibility for the Department's counterintelligence and security programs.

Let me begin by describing in quantitative terms the enormity of the security problem faced by the Department. As of the first of April, we had a total of 4.3 million persons cleared for some form of access to classified information.

Of these, 2.9 million were civilian or military employees of the Department; and 1.4 million were employees of the more than 14,000 defense contractors with some form of security clearance.

While by far most of these cleared persons are physically within the United States, DOD has some form of official presence within 120 countries around the world.

Last year these cleared personnel created and handled an estimated 16 million classified documents, of varying degrees of sensitivity.

DOD personnel, installations, and contractors have long been targets of espionage efforts as well as other types of technical collection efforts undertaken by our adversaries. For the most part, our people and our contractors are rather easily identified by hostile intelligence, both in terms of where they work and the sorts of activities in which they are likely to be engaged.

We receive in the neighborhood of 600 reports annually of possible contacts of hostile intelligence services with DOD personnel. All, I might add, are reviewed and investigated as appropriate.

Unfortunately, we must also recognize that not all espionage is instigated by the other side. We have occasional instances where Defense Department employees and contractors initiate the contacts themselves, offering to sell classified information to which they have access.

When weighed against the vast numbers of cleared people, however, the number who agree to participate in, or initiate, espionage activities is infinitesimally small. But it is equally true that one person with the right access may be capable of compromising military systems that cost the United States literally millions, if not billions of dollars to develop and produce.

This may lead to actions to counter the latest U.S. military hardware or the latest U.S. strategy. And so, from our standpoint, even one case is too many.

So, what do we do to prevent and detect these efforts?

There are defense directives and regulations which address this subject that would literally reach from the floor to the ceiling of this hearing room. They cover virtually every aspect one can imagine to protect classified information from unauthorized disclosure.

Without attempting to describe them in detail, let me identify conceptually the sorts of programs encompassed here.

First, there are policies governing the classification of information in the interests of national security. These are set forth in Executive Order 12356 which applies to all departments and agencies of the executive branch, as well as its contractors. Flowing from this basic document are rules which apply to the marking, handling, reproduction, accountability, transmission, storage, and destruction of such information.

These policies encompass not only requirements to lock classified information in safes, as one might expect, they also cover such things as the kinds of telephones that one might use to discuss classified information; how electronic equipment processing classified information must be shielded to prevent emanations leaving the area; what methods are acceptable for destroying classified information; how information to be released to the public must be screened for classified information; whose permission must you have before you can classify or reproduce a classified document; what you have to do before you can share classified information with an allied Government; when you have to have areas swept electronically to determine the presence of listening devices.

In short, virtually every circumstance one can think of, in terms of precluding the possible exposure of classified information to unauthorized persons, is treated in the regulations of the Department.

The second major area of policy—apart from how classified information is identified and physically protected—governs who shall have access to it.

In general, access can be granted to someone whom the Department has determined to be trustworthy and has a security clearance, and who has a "Need-to-Know" information classified at a particular level in connection with his employment with DOD, or his performance on a DOD contract.

A clearance is normally requested by the employing office of a DOD component, or by a cleared defense contractor, who must certify that the individual involved has a need to access classified information at the level of the clearance being requested.

The request for investigation goes to the Defense Investigative Service, whose 1,555 investigators carry out all background checks for the Department of Defense.

The checks performed in a particular case depend upon the level of clearance requested. In general, persons receiving a top secret clearance, and those requiring special intelligence accesses are subject to a full field investigation, while secret and confidential clearances are based upon a so-called National Agency Check, which amounts to a check of pertinent Federal agency files, including the FBI, for indications of derogatory information concerning the subject.

Once the field investigation or National Agency Check has been completed, the results are provided to the requesting DOD component, or in the case of defense contractors, the Defense Industrial Security Clearance Office, for a decision whether a clearance should be issued the individual.

The process does not end there, however. Since 1983, comprehensive reinvestigations are being done for those with top secret and special intelligence accesses. For the last 2 years, DIS has done roughly 40,000 of these.

Supervisors of cleared employees both in DOD and in industry also have a continuing responsibility to identify and report facts that become known to them concerning their cleared employees which may have security significance. All such reports are investigated by DIS or the military services, as may be appropriate.

There are also requirements in DOD and in defense industry for periodic security awareness briefings, when cleared employees are advised of the threat posed by hostile intelligence collection and what to do should they be contacted.

Approximately 1.3 million persons were reached by such briefings last year. They were supplemented in defense industry by FBI briefings, as well.

In addition to these measures which have general applicability to all classified programs, we also have rules that apply to especially sensitive classified information protected within so-called Special Access Programs.

Executive Order 12356 authorizes the Secretary of Defense and the Secretaries of the military departments to create special security compartments to protect unusually sensitive classified information. At a minimum, only persons who have been specifically designated for the particular information are eligible for access.

In essence, the special access program is a way of institutionalizing the "Need-to-Know" principle. Additional security measures not otherwise required with respect to normal classified information are typically required, tailored to meet the particular needs of the program in question.

I should also mention with respect to these special access programs that DOD is currently implementing a test program utilizing a limited polygraph examination as a condition of access to such programs.

As you know, Congress authorized DOD to conduct such a test of the polygraph—limited to 3,500 persons—as part of last year's Defense Authorization Act. This test was extended in the fiscal year 1986 authorization bill, passed by the Senate, to the end of fiscal year 1986.

The third major area of policy deals with enforcement of the rules. I have already mentioned the fact that the system itself has a built-in self-policing aspect. All supervisors of cleared personnel are charged with the responsibility for identifying and reporting information of security significance concerning their employees.

Security violations also may be reported on an anonymous basis over the DOD hotline, established and operated by the DOD Inspector General. Reports made in accordance with both procedures are investigated by the Defense Investigative Service, or the military services as may be appropriate.

There are also a voluminous number of security inspections which periodically occur; 26,000 were done within DOD in 1984.

In addition, all defense contractors who hold security clearances are periodically inspected by the Defense Investigative Service to determine compliance with DOD policy.

With respect to detecting actual instances of espionage, each of the military departments has a counterintelligence investigative agency responsible for its particular branch of service.

In the Army, the responsibility rests with the Army Intelligence and Security Command.

In Navy, with the Naval Investigative Service.

And in the Air Force, with the Air Force Office of Special Investigations.

Each of these agencies conducts counterintelligence investigations and operations designed to detect spies within their ranks. In the United States, all of these activities are undertaken jointly with the FBI. Overseas, they are coordinated with the CIA.

The subcommittee should also recognize that our investigative jurisdiction in these matters is limited to military personnel. The FBI has primary investigative jurisdiction over all Defense Department civilian personnel and contractors, and they coordinate such activities with my office.

Finally, we receive critical support from the FBI, and occasionally from other agencies, in terms of identifying DOD personnel who may be involved in espionage. It is very much a cooperative effort.

Unfortunately, despite all of this, we have people who decide to commit espionage and manage to escape detection for some period of time. What can be done to prevent this?

Secretary Weinberger recently established a senior DOD commission, to be chaired by recently retired Deputy Under Secretary of Defense for Policy, Gen. Richard G. Stilwell, to examine what might be learned from the *Walker* case and develop recommendations for the Secretary.

There are obviously things that might be done to reduce the exposure of classified information in general. Reducing the numbers of people with clearances, as the Secretary has already directed, is one such action and we are pursuing the goal of further reductions.

Obviously, the object is to accomplish the defense mission with as few cleared people as necessary.

Bringing a greater degree of discipline to the classification system is another. We are now developing new procedures to reduce the numbers of classified documents being created—particularly in the higher classification categories—and in return hope to accomplish better protection for those that are classified.

We are also looking at ways to improve the investigations done on those who require clearances, including, as I mentioned, how the polygraph should be used to supplement such investigations.

The Department is now urging Congress to provide statutory authority for our investigators doing background investigations, to obtain criminal history data from State and local jurisdictions where such access is presently denied them.

I understand Senator Nunn introduced such a bill yesterday. We are indebted to you, sir, for that and we hope it will be enacted by the Congress.

There is also more that can be done to improve the odds that espionage will be detected. An increased awareness on the part of supervisors and fellow employees to indicators of espionage would, in my view, produce particular dividends.

Perhaps, if nothing else, the *Walker* case and what we know of it to date, will demonstrate to our employees that no office or no activity is immune from this threat.

The resources devoted to the counterintelligence efforts of the Government also clearly impact the problem. These resources have increased substantially in recent years, and at the same time we have been catching more people who are involved, or attempting to become involved, in espionage.

Still, the assignment of the U.S. counterintelligence community to keep track of the activities of known or suspected intelligence operatives within the United States is a formidable one. Not only are resources important in this regard, but the legal confines in which hostile intelligence agents must carry out their activities within the United States are an equally important part of the equation.

That environment, fortunately, became more restrictive in recent years, and several proposals are currently pending in Congress to limit the capabilities of hostile intelligence within the United States still further.

Which brings me to S. 1301, itself a proposal to improve DOD counterintelligence capabilities. Mr. Cox will cover the provisions of the bill relating to new penalties for espionage under the Uniform Code of Military Justice; I will confine my comments to the other provisions.

I can quickly dispense with sections 3 and 4 of the bill, which require the Secretary to submit reports within 180 days to the Congress regarding:

First, the capabilities of the military departments and the Office of the Secretary of Defense to conduct counterintelligence operations; and

Second, his plans for reducing the numbers of security clearances within the Department.

We have no objections to these requirements.

Section 6 of the bill does raise the issue, however, of how broadly the polygraph will be used in determining the access of DOD employees and contractors to classified information.

Subsection (a) would mandate a limited polygraph examination as a condition of obtaining access to sensitive compartmented information—which is a euphemism for information revealing intelligence sources and methods—and require such examinations to be given aperiodically thereafter.

Subsection (b) would provide the Secretary with discretionary authority to require limited polygraph examinations as a condition of access to other categories of classified information, and to utilize such examinations aperiodically thereafter to determine continued access.

If these two subsections of the bill were adopted, they would appear to make a change of course over what this committee and the Congress had previously authorized.

Without recounting the 2 years of discussions that went into working out a consensus on the issue, let me simply remind the subcommittee that in the fiscal year 1985 DOD Authorization Act, this committee inserted a provision that authorized the Department to undertake a test program utilizing a limited counterintelligence polygraph examination for persons who required access to highly classified information protected within the so-called special access programs.

The test was initially to have run through September of this year, and would be limited to 3,500 persons. At the end of the test, we were to report the results and decide the shape of any future program.

Several weeks ago, this committee voted to extend the test program at the same 3,500 level through to September 1986. This extension was agreed to by the Department, and it was included in the bill which recently passed the Senate.

All of this came before the *Walker* case, however, and there have been a great many people, both inside the Department and outside the Department, urging that we should make greater use of the polygraph in our security programs.

And so, the issues posed by S. 1301 are whether the test program approach be modified, and if so how?

On the first issue, we must defer to the committee. The Department accepted the committee's proposal for such a test program, and we are prepared to see it through.

If, on the other hand, the Congress now wants us to conduct additional examinations covering additional categories of cleared personnel, or, at the conclusion of the test, begin implementing such a program, we are prepared to adopt this course.

As a practical matter, whatever course is taken, the number of polygraph examinations that are administered before the end of fiscal year 1986 are not likely to exceed 3,500. We simply do not have enough trained polygraph operators and polygraph instruments to implement such a program on a more expanded scale at this time.

Moreover, our capability to train and equip such operators is at this juncture relatively limited. Our training facilities must be considerably expanded and our inventory of polygraph instruments considerably increased before any large-scale use of polygraph examinations will be feasible.

If the committee decides that DOD should be authorized now, or at the conclusion of the test program, to implement a polygraph program on a broader scale, then it should also consider whether the "broader scale" set forth in S. 1301 is the best alternative.

As you recall, S. 1301 would require mandatory polygraphs for SCI access, and permit the Secretary discretionary authority to use such examinations as a condition of access to other types of classified information.

Our problem with this formulation is that since there are over 100,000 people in defense with SCI access, and polygraph examinations would be required by law for such persons, it would take us several years, given our limited number of trained operators, before we could consider using the polygraph in other programs of equal, if not greater, sensitivity.

We would, therefore, prefer a greater degree of discretion in terms of how limited polygraphs will be employed.

As an alternative, as to how we should proceed from here we would suggest you consider the following approach:

First, DOD would continue to implement and complete the already authorized test program, and report its results to the Congress as directed.

Second, DOD would expand its training facilities equipment in fiscal year 1986 necessary for a continuation of the program after fiscal year 1986.

Third, at the end of the test program, DOD, in consultation with the committee, would adjust its program for the future based upon its experience with the 3,500-person test, and the recommendations of the Stilwell Commission.

Fourth, at the conclusion of the test, however, the committee would permit the Secretary to develop and operate the program from that point in the manner in which he determined provided the greatest degree of deterrence and protection, given the number of trained operators then available.

This would be done with whatever degree of committee involvement you wished to have, but we would not be tied to a statutory requirement to polygraph large numbers of persons within specific categories, at particular times, such as set forth in S. 1301.

Fifth, close and continuing congressional oversight would be involved in monitoring the program as it develops over time.

I believe this approach offers many advantages without upsetting what has already been carefully worked out. In particular, it would mean there are the necessary resources available to implement the program at the time the test has run.

It would also leave the Secretary in a position to apply such resources where he felt they would do the most good. And, it would allow us to factor in both the test experience and the recommendations of the Stilwell Commission and the views of the subcommittee into any future program.

In conclusion, let me say we appreciate the concerns of this subcommittee that we do all within our power to prevent and detect espionage undertaken against the Department and the United States. Obviously, we share those concerns.

We also appreciate the desire of Senator Gramm and others in Congress who want to give the Secretary what he needs to do this job. The polygraph is one technique which clearly merits use within the overall program.

There is, however, I am afraid, no panacea. Whatever we may do, there will be other cases—perhaps not as many, perhaps not as serious, hopefully not as drawn out as has recently come to light.

It is the challenge for all of us involved in this area to minimize their occurrence within the limits of our resources and consistent with the values and principles of a free society.

I will be glad to answer any questions you may have.

Senator WILSON. Thank you very much, Mr. Snider.

We have been joined by Senators Cohen and Denton, regular members of the subcommittee.

Gentlemen, we are going to have 10-minute rounds to begin with.

Mr. Snider, I must say I find amazing some of your figures concerning the number of personnel who have clearance for access to classified information. Your information indicates that 2.9 million military personnel and civilian employees of the Department presently have such clearance.

During fiscal year 1985 the Department has only authorized 3.2 million military and civilian personnel. That means that more than 90 percent of the personnel in the Department have some form of security clearance.

Is there really a need for 90 percent of personnel to have security clearances?

I find that mind-boggling. If we were to apply the provisions of S. 1301 to the numbers you have provided, and you are right to remind us of our earlier judgment with regard to the polygraph, and, if there are 100,000 of those 2.9 million who have SCI access that would require mandatory application of the polygraph, that would leave you faced with an impossible burden given the resources that you have.

That 2.9 million seems excessive. I would be grateful if you would explain really how this situation came about and, furthermore, if you would explain to the subcommittee whatever details you can about how the Secretary intends to comply with the requirement in the bill that he detail his plans for a reduction in the number of clearances within the Department.

Later, we will need to discuss, although the bill does not describe it, the reduction of clearances on the part of contractor employees.

Let us deal with DOD directly at this point. It is clear that we are going to have to shrink the number of clearances. The clearances and polygraph resources don't fit. Even if we weren't talking about the polygraph, what about this 2.9 million?

Mr. SNIDER. I think you are quite right. There are too many people with clearances in DOD and in defense industry. How many, I really don't think anyone knows the answer to, but clearly there are a lot of people out there who don't need access to classified information, but for one reason or another have clearances.

As I mentioned in my statement, the Secretary imposed a 10-percent reduction a few weeks ago in the number of clearances across-the-board to be achieved by October 1.

Presumably on that date we will be talking about 80 percent, using your figure, but even this is still too high.

Why did all of this come about? Well, we have seen a tremendous increase in industrial clearances. That is where we have seen most of the increase take place in the last 10 years in terms of the number of people requiring clearances.

It stems from the fact that so much defense contracting now is classified. It also stems from our competitive procedures which require any firm who wants to bid on a classified contract to receive a security clearance before he submits a bid on that contract.

So, given the high tech nature of the equipment and hardware systems that are being manufactured, quite a bit of which is classified, it requires clearances for the people who produce it, who operate it, who maintain it.

We just don't have tanks any longer that are heaps of iron and steel. They have laser rangefinders and digital equipment built into them which are classified. So, all of the tank operators have to have clearances.

Senator WILSON. Let us stipulate to the fact that increasingly complex technology has given some impetus to this. I think the real question is: Has there been routine certification, both by defense contractors with regard to their employees and by the Department itself, with regard to its employees, military and civilian? Is it essential that all these people have this clearance? Are we simply going to have to require then a far greater discipline and subject them to the kind of techniques that will give some assurance that our security won't be breached?

Mr. SNIDER. Just to clarify, we wouldn't give routine certifications as a means of granting clearances, but I think the problem you are getting at is that we have not put any limits or restrictions either on contractors or defense components in terms of the number of clearances they can request.

Whatever they have requested heretofore, the Defense Investigative Service has simply run an investigation and the results are adjudicated.

I think the Secretary's action, which included not only a reduction in issuing clearances, but a reduction by 10 percent in the number of requests for new investigations in fiscal year 1986 will force DOD components and industry to manage the requests they are submitting.

I think we will get much better assurance that in fact the people who are being put in actually need clearances.

Senator WILSON. If the bill is adopted, the requirement is that the Secretary make plans for this reporting requirement within 180 days.

In your testimony you stated there is no objection to that. I will simply take that at face value. I have asked for some detail on how it is going to be done. But if you feel there is no objection or problem, then I will accept that.

If you feel there is, now is the time to speak or the Secretary will have a problem down the road, obviously.

Mr. SNIDER. There is no objection. In fact, we will provide a report to the subcommittee whether the bill is passed or not, if you want us to.

Senator WILSON. We are asking you to provide useful information so that we can impose a reasonable requirement.

Mr. Snider, you indicated that the 1,555 investigators of the Defense Investigative Service carry out all the background checks for the Department of Defense. There have been numerous press reports in recent weeks about gigantic backlogs of these investigations.

Furthermore, you point out in your testimony that since 1983, comprehensive reinvestigations are required of those personnel with top secret and special intelligence access clearance and that DIS has done roughly 40,000 reinvestigations in the last 2 years; 40,000 is only about 5 percent of the some 730,000 existing clearances for access to top secret or special intelligence access. At that rate it is going to take you 40 years to do the required investigations.

In your report to us obviously you are going to call for increased resources. I will simply invite your comment on it because it seems to me that that is almost a rhetorical question.

Mr. SNIDER. Let me clarify one thing. The number involved here in the top secret and SCI area who have reached the point where they need a 5-year update is around 279,000. It is not quite as bad as 700,000, the total population of top secret and SCI access.

Even at that, you are quite right; we have a sizable backlog in terms of doing the periodic reinvestigations on schedule.

We do think that the reductions in the number of investigations that are going to be requested over fiscal year 1986 is going to mean that we will have more investigators to do periodic reinvestigations, and our rate of accomplishing these reinvestigations will increase over time.

We obviously would like to get more resources for the Defense Investigative Service to reduce this backlog, to eliminate it, so that we can keep on schedule.

Senator WILSON. Thank you, sir. My time has expired.

Senator Nunn.

Senator NUNN. Thank you, Mr. Chairman.

I have a couple of questions on the overall question of security clearance.

Is it true, Mr. Snider, that DIS does not charge anything for security clearance checks?

Mr. SNIDER. That is correct.

Senator NUNN. Are you reexamining that? It seems to me that if we really believe in the system in the Government as well as the free enterprise system, if you charge for something, you have fewer people than if you give it away free.

Doesn't it stand to reason if you started charging, as the Office of Personnel Management already charges for their security clearance checks, that you would have fewer requests?

Mr. SNIDER. We have looked at that before and our conclusion has always been that it just entails much more administrative cost in terms of other DOD components having to budget for this function separately, rather than have the Defense Investigative Service carry it out for the Department as a whole.

The problem is that DIS requirements have been so enormous in recent years they just haven't budgeted enough resources.

Senator NUNN. The point is no matter what you tell somebody, if you are giving something away, if they can get as many checks as they want and it doesn't come out of their budget or the contractor does not have to pay for it, it stands to reason there will not be any serious inhibition. First, if you charge a reasonable fee it represents an income for the Department of Defense Investigative Service and could conceivably be used to beef up resources there.

Second, it acts as a disincentive.

Right now you have OPM that charges for their security clearances. They charge other agencies. DIS doesn't. So, there is a direct incentive for an agency that has any kind of budget problem to go to DIS.

I think you need to look at these numbers.

Mr. SNIDER. We will do that.

Senator NUNN. On the polygraph test, how are you conducting the ones that you are doing now, the 3,500?

Can you give a general description of what you are doing now, how you are going about it?

Mr. SNIDER. Sure. To date there have only been roughly 300 exams given. They have been within programs that have been nominated by the Secretaries in the military departments, special access programs, and each of the military services' investigative agencies that have trained polygraph examiners on board are being asked to contribute their part and help carry out this test program.

They are intentionally taking it out of the existing pool of examiners that are normally used for criminal investigations.

We expect to have another 300 examinations done by the end of this fiscal year and the balance done in the next year to come up to the 3,500 test limit.

Each of the military departments has nominated programs for the test. Defense Intelligence Agency has also nominated its intelligence positions for purposes of the test. We are ready to carry it out and we will have enough to meet the test, but it will be done within existing resources.

Senator NUNN. How many operators do you have that qualify for polygraph examining to administer the 3,500 tests?

Mr. SNIDER. I am not sure I understood your question.

Senator NUNN. To administer 3,500 tests, you have 3,500 tests you are permitted under the test program?

Mr. SNIDER. Right.

Senator NUNN. How many polygraph experts do you have to have to be able to administer that number of tests?

Mr. DONNELLY. Each one does 200 a year, 250 a year, or so.

Mr. SNIDER. Probably in man-years about 20 examiners.

Senator NUNN. Twenty examiners?

Mr. SNIDER. That is a rough approximation. We figure one examiner can do 250 exams a year. That is for planning purposes.

Senator NUNN. Do you have the capacity?

I believe your testimony here regarding the bill that we are having a hearing on is that you really can't expand that beyond what you are doing now up through at least fiscal year 1986.

Is that what you are saying?

Mr. SNIDER. That is correct.

Senator NUNN. What are the limiting factors that keep you from expanding?

Mr. SNIDER. The limiting factor is our inability to train qualified examiners in a very short period of time. The Army is executive agent for the Department and runs the Department's polygraph school. It has a capability of training only 48 examiners a year, and has a very small staff of seven people.

In addition to the requirements that DOD has, the school also trains polygraph examiners for seven other Federal agencies.

Out of the last couple of graduating classes, half have been polygraph examiners that DOD is training for other agencies.

Senator NUNN. You are basically saying no matter what you have in authority, you are not able to carry out more than what you are now planning in the next fiscal year?

Mr. SNIDER. Yes, since we essentially must take the additional examination out of hide, so to speak, from those doing criminal work.

Senator NUNN. What if you are given authority and money to go out and hire other people and beef up your training program, could you do that?

Mr. SNIDER. We could certainly beef up the training program. As my statement suggested, that is precisely what we would like to do.

We would like to expand the capacity of the school. We have not seriously considered contracting out for this kind of service, nor would we, I think, consider that very seriously.

Senator NUNN. Why is that?

Mr. SNIDER. I think the basic reason is quality control over the polygraph examiners and the examination process. Having your own employees do it is essential.

I think if in fact we contracted out, we would lose a great deal of control over that process. It is in a very important area to utilize people with good judgment, good training.

Senator NUNN. I agree with that. You are absolutely right.

Senator COHEN. If you will yield on that point, as I recall, John Walker had his own polygraph examination division within his firm so that those Navy personnel would be in charge of drug abuse, they couldn't be polygraphed by the DOD, they could be polygraphed by John Walker's outfit to find out whether they could erect an adequate defense.

Walker, himself, could take that polygraph information and find more recruits in terms of people who had vulnerability within the services.

Senator NUNN. In section 6(a) of the Gramm bill, the Secretary of Defense is required to use these examinations to determine initial eligibility for access to sensitive compartmented information.

Now, in the course of the year, how many persons do you clear for access to sensitive compartmented information?

Mr. SNIDER. It is roughly 8,000, I am told.

Senator NUNN. 8,000 per year?

Mr. SNIDER. Yes, sir. This would not be including NSA. It would be including the rest of the Defense Department.

Senator NUNN. How many do you have that are already cleared? What is the number cleared for sensitive compartmented information?

Mr. SNIDER. 102,000, approximately.

Senator NUNN. If you were going to actually implement 6(a) fully, you have 102,000, and would have 8,000 that would be cleared. I am not sure, Senator Gramm could tell us, the other section here also requires periodic use to determine continued eligibility of such persons.

I am not sure whether that is over 1 year or 2 years, but let us assume for the purpose of getting a fixed number of polygraph operators, you need, if you did implement that, let us say over a 2-year period, you have 8,000 new ones each year, that is eight times two, 16. You have 102,000 backlog, that would be 118,000 people.

Now, based on your formula of 250 people per year, how many polygraph examiners would you have?

Mr. SNIDER. I don't have my calculator, but it is a matter of dividing 250 into that.

Senator NUNN. 250 into 118,000. That is about 472.

If you do not want to go outside, if you beef up your training program, how long would it take to get into a position to carry that out and what are you asking for in additional resources?

Mr. SNIDER. What we are suggesting, we have taken a look at this, what we would like to do at least is adopt this for planning purposes, to expand the capability of the school to train 108 examiners a year as opposed to 48 examiners a year.

We think, given the attrition that we ordinarily have in the program in terms of polygraph examiners leaving the program, requests from other agencies that we train their people, we think if we had 108 coming out of there every year, it would give us enough capability to establish a credible program of the sort we are talking about here.

Senator NUNN. It would take a long time to get that?

Mr. SNIDER. Yes, sir.

Senator NUNN. One other question.

You said there are other areas more important or just as important as sensitive compartmented information.

What other areas are you referring to that are just as important and what is the number of people involved here?

Mr. **Snider**. Apart from SCI access, we have special access programs that cover primarily R&D programs which DOD considers extremely important.

We also have operational plans and programs that are in fact encompassed within special access programs that again we consider every bit as sensitive as intelligence reports or intelligence sources and methods.

Senator **Nunn**. What are the numbers?

Mr. **Snider**. There are approximately 43,000 defense employees other than those with SCI access that are cleared for some form of special access program. Some also have SCI access.

Senator **Nunn**. 40,000?

Mr. **Snider**. 43,000. Other than what is in SCI access programs.

Senator **Nunn**. That is total, those other two categories combined?

Mr. **Snider**. Yes, sir.

Senator **Nunn**. Does that include defense contractors?

Mr. **Snider**. It does include defense contractors.

Senator **Nunn**. If you put everything that you felt was equal to the SCI clearance in one box, you would have 118,000 plus 43,000, about 151,000 people in that category of very important?

Mr. **Snider**. That is correct. Or course, this does not even include programs that are classified top secret or secret that are again very sensitive.

We run most of our counterintelligence operations and HUMINT operations at the secret level, for example, and these are not even contained in a special access program.

Senator **Nunn**. Thank you, Mr. Chairman.

Senator **Wilson**. Thank you, Senator Nunn.

Senator Cohen.

Senator **Cohen**. I have a couple of questions and will then yield to Senator Gramm.

What has been your experience to date? How effective has it been in detecting those who might be susceptible or who might have been compromised prior to having access to the information?

Mr. **Snider**. We think it can be a very effective tool with qualified examiners, up-to-date equipment and quality control procedures, with supervision over the whole process. We think it has been very effective.

It has been used in NSA for years, as you know, as a condition for employment there. All applicants for employment in NSA take the polygraph examination. NSA has found it to be unusually useful in terms of producing derogatory information about a particular subject through his own admissions that would otherwise never come out in the process of the background investigation.

They have even had a number of cases where they have found people who were apparently sent to NSA to commit espionage, to, in fact, penetrate that Agency.

We also use it other than in NSA primarily in the criminal area, in assisting in criminal investigations.

I ought to point out that whenever it is used, the results of the polygraph are never taken solely as a basis for doing anything. It supplements other investigations that the Department does. We wouldn't take action based solely on the results of the polygraph.

Senator COHEN. Are there any restrictions on the type of questions that are asked?

Mr. SNIDER. As far as NSA is concerned, it is a full lifestyle polygraph for employment in NSA. As part of our counterintelligence test program, however, we have a very limited set of questions, essentially asking the subject if he is a spy, does he know anyone who is a spy, getting him to answer that kind of direct question on the polygraph.

Of course, the criminal investigation is related to whatever the subject or issue is.

Senator COHEN. Let me ask you a question.

If you ask, do you know a spy or anyone who knows a spy, what about the type of personal questions that might make that individual more susceptible to being blackmailed?

Mr. SNIDER. We do not cover those in the test program. It is limited only to the questions I mentioned. If we had a showing of deception, I am sure the examiner would then ask the person who he was examining what he thought was the basis for his reaction. It may get into other subject areas.

Senator COHEN. I am thinking more along the lines of what happened with an FBI agent on the west coast, along the lines of what has been happening with respect to these spies, whether for ideological reasons or whether for greed or money.

Is your polygraph detector test going to pickup the kind of vulnerability that might lend itself to an individual like *Walker* or anybody else?

Is it so helpful that you can ask Senator Nunn, Senator Gramm, do you know any spies?

We know a lot of people down at the Embassy who could be spies.

Senator NUNN. I know some Senators who have written about it.

Senator COHEN. That is not necessarily going to help you out.

Mr. SNIDER. I understand what you are saying. You are probably right.

On the other hand, when you start asking personal questions, it raises a lot of additional problems, as you can appreciate, for our employees. We limit ourselves to security questions.

Senator COHEN. We hear a lot about exit polls in California.

What about exit polygraphs?

Senator Nunn and I serve on the Governmental Affairs Committee and we recently conducted hearings, Christopher Boyce being the most celebrated witness appearing before us. One of his recommendations is not periodic polygraphs, but exit polygraphs; people who were in the service or worked for a defense contractor knew that before they could leave one position and go on to another, they would have to submit to a polygraph test.

Mr. SNIDER. I think that might be a pretty strong deterrent to people who think of commiting espionage.

On the other hand, by waiting until termination of employment you put yourself in a position of having lost the information you are worried about.

Senator **Cohen**. That could be combined with the other.

Senator **Gramm**. If he knew it was coming, it would be a deterrent.

Senator **Cohen**. Finally, should we have special clearance procedures for those who have crypto specialties?

Mr. **Snider**. That is an interesting question.

The National Security Agency thinks we should. There used to be, in fact, a special designation if you handled crypto materials, or had crypto access, but the old program of crypto access special designations did not involve special clearance requirements.

As I understand it, it was a simple matter of having a commanding officer or employer look at a particular employee and decide he was a trustworthy person and designate him as a crypto custodian. So, we weren't getting much more protection.

Senator **Cohen**. *Walker* was patriotic. Isn't that a classic case. What can you judge by looks?

Mr. **Snider**. Not very much.

Senator **Cohen**. I think it is something you ought to look at anyway.

Mr. **Snider**. We will be looking at that.

Senator **Wilson**. Thank you, Senator Cohen.

Senator Bingaman.

Senator **Bingaman**. Thank you, Mr. Chairman.

I gather from your testimony, Mr. Snider, your position is that although the Defense Department was in general agreement with the test program that the committee set out in the Defense authorization bill this year, that as a result of the *Walker* case, you now feel that that is not adequate and that you need additional authority for polygraphs?

Is that right?

Mr. **Snider**. I am not sure that is quite right. I think it has always been our intention that there would be some form of program that would continue after the test.

We are certainly willing to look at the results of the test in terms of calibrating the system for the future. We are prepared to go with the test.

We would, on the other hand, like to have in the future some sort of authority, or at least agreement on the part of the Congress, that this is something that should be part of our security program.

Senator **Bingaman**. What I am getting at is for fiscal year 1986 we had thought we had an agreement by the Defense Department that the test program of 3,500 a year was adequate and now I am unsure as to whether you believe that that is adequate for fiscal year 1986.

Mr. **Snider**. It is adequate for fiscal year 1986 if for no other reason than we can't do any more than what has been proposed in the test already. If we had the capability in place to do more, I would favor a larger number. We just simply don't have the capability.

Senator **Bingaman**. When is General Stilwell's Commission to report on this?

Mr. **Snider**. General Stilwell's Commission is to report within 120 days of the date of his charter, in fact. It will be approximately 4 months.

Senator **Bingaman**. It is your thought, based on what you know now, that you need to expand or you would like to expand your use of the polygraph even before his report is complete?

Mr. **Snider**. As I said in my statement, we would like to go ahead and proceed with the test and then look at the expansion at the end of it in light of his Commission's recommendations as well as where we are in terms of having trained operators available.

It will take some time just to expand our training facilities. We recognize this.

Senator **Bingaman**. Are there examples where people have passed these counterintelligence polygraph exams which are given to ask a person if they are a spy and then they turned out to be spies?

Mr. **Snider**. Not that I am aware of.

Senator **Bingaman**. I thought I heard about some Czech emigres who the CIA polygraphed who turned out to be a spy, although he had successfully passed the exam.

Do you know anything about that?

Mr. **Donnelly**. The Czechs you are referring to were polygraphed when they were interpreters for the CIA. I understand that the reexamination of those charts changed the minds of the experts and the experts misread the charts at the time.

Senator **Bingaman**. So, after he turned out to be a spy, they went back to tell that they should have known he was a spy?

Mr. **Donnelly**. Some of the polygraph operators say you don't beat the machine, you beat the operator.

Senator **Bingaman**. I know this is sort of the purpose of the test program, but do you have any sense for the extent of false negatives where a person does OK, comes out clean on the polygraph, but later turns out to be a spy?

Do you have any preliminary thoughts as to the extent of the false negative problem or the false positive problem?

Mr. **Donnelly**. I don't think we have any statistical basis to make any prediction on that. We are satisfied that the number of false positives would be very limited, provided we have well trained people, have good quality control backup and separate people looking at the chart after the operator looks at the chart.

Senator **Bingaman**. Let me ask something that you said, Mr. Snider, a little earlier that caught my attention.

You said that a tank operator needs a clearance because the tank is equipped with high technology devices.

I am just wondering, if you carry that to its logical extreme, everybody in the world ought to be polygraphed these days because you have such access to high technology.

Is that the basis that anybody who comes in contact with high technology machinery, even to operate it, needs a clearance?

Mr. **Snider**. Well, most of the military department manuals on how to operate and repair their equipment are in fact classified. Some people who have to do that require clearances to see the manual.

Getting back to your question, we do not necessarily equate a security clearance, for example, at the confidential level with a requirement for a polygraph. I think we have to use more judgment than that in terms of protecting the most sensitive information we hold, given our limited resources.

Senator **Bingaman**. Let me characterize the concern I have and you tell me if I am wrong or right.

I think the problem is that we have too many people who are cleared for classification. We have too much material that is classified.

I am concerned that with the best of intentions the suggestion that we greatly expand the use of the polygraph may just add another layer of too much checking on too many people whom we should not have to check on in the first place because they should not have access to this information.

Is the solution to the problem we have, that the *Walker* case highlights or any of the rest of it, more polygraph examiners and more machines? Is that the solution?

Mr. **Snider**. Let me say this. I agree with you there are too many people cleared, and there are too many classified documents.

I also think that we do need to be able to use the polygraph, particularly in areas of extreme sensitivity, for programs that if they are penetrated, will cause serious harm to the country, to the Defense Department's programs. It is a tool, a useful tool.

Senator **Bingaman**. You don't see the present law as a major impediment to your ability to do that right now?

Mr. **Snider**. No, the only impediment we have in the law is the restriction in the authorization bill.

Senator **Bingaman**. Restriction on the amount of money you have; is that what you are saying?

Mr. **Snider**. The restriction that confines us to doing a test program. That is the only new use we can make of the polygraph in this fiscal year.

Senator **Bingaman**. You tell me even if you had authority to make more use of it, you don't have the people and you haven't asked for resources to do that?

Mr. **Snider**. To date, that is correct.

Senator **Bingaman**. So that the real limitation on you is the lack of resources and those are resources you have not requested of the Congress?

Mr. **Snider**. Yes, lack of resources. We want to make sure what resources we get are applied prudently within the program where we will see the greatest benefits. We are not trying to polygraph everyone.

Senator **Bingaman**. Obviously, you want to do it effectively.

Thank you very much.

Senator **Wilson**. Thank you very much, Senator Bingaman.

We will be in recess until 3:30.

[Recess.]

Senator **Wilson**. The subcommittee will reconvene.

Our subject is S. 1301.

The Chair will recognize the distinguished ranking member, Senator Glenn, for a statement and questions.

Senator **Glenn**. Thank you, Mr. Chairman.

I would like to ask unanimous consent that my opening statement be entered into the record as though delivered.

It is a statement of my concern about this particular area. I will not bother to read it here, but I would ask that it be entered into the record.

Senator **Wilson**. It will be entered into the record in its entirety.

[The prepared statement of Senator Glenn follows:]

PREPARED STATEMENT OF SENATOR JOHN GLENN

Mr. Chairman, like all Americans I have been very concerned by the revelations of spying and espionage that have come to light as a result of the Walker espionage case in the last few weeks. The full damage to our national security as a result of the activities of this spy ring is still being assessed, but there is no doubt that this damage has been severe.

Unfortunately, this spy case just underscores the conclusions of the 10 months of hearings and investigations that we recently completed on the Government Operations Permanent Subcommittee on Investigations: the Soviet counterintelligence threat is real and pervasive; we need to improve our own counterintelligence capabilities to counter this threat; and our procedures for granting access to sensitive classified information to individuals in and out of government need to be tightened considerably.

The bill we are considering today, which has apparently been drawn up as a response to the Walker spy case, includes a number of very far-reaching provisions:

The bill includes peacetime espionage under the Uniform Code of Military Justice and prescribes a sentence of death or mandatory life imprisonment for any military member convicted in an espionage case involving a communist country.

The bill requires the Secretary of Defense to use polygraph examinations in granting individuals access to sensitive compartmented information, and grants authority for the Secretary to require polygraph use in determining access to *any* classified information.

Finally, the bill amends the Federal Criminal Statutes in title 18 of the United States Code to require a mandatory sentence of death or life imprisonment for any person convicted of espionage on behalf of a communist country, and establishes procedures for federal courts to use in deciding whether to apply the death penalty. I assume this last provision will require sequential referral to the Judiciary Committee.

Mr. Chairman, this bill raises many complicated and controversial issues. In my view, in order for us to act in a deliberate and responsible manner on this legislation the Subcommittee will have to hold a series of hearings on this bill. We will need to hear from the Department of Defense, and possibly representatives of the military services, on their views of this legislation. We will need to hear from the Justice Department. And we will also want to call outside witnesses, including experts in constitutional law, to give us their views on this bill.

I am very concerned about the whole subject of Soviet espionage and our ability to counter this threat. But this is too important a subject to rush to judgement on a wave of public concern. I will be glad to work with the Chairman of the Subcommittee in the coming weeks in drawing up and participating in a series of hearings that will allow a full and complete consideration of the issues raised in the legislation before the Subcommittee.

Mr. Chairman, I look forward to the witnesses' testimony.

Senator **Glenn**. What is your reliability on polygraph?

I am concerned about the penalties in this bill, I am not necessarily against them, but I want to make sure we get all these things adequately attended to.

Mr. **Snider**. You can read a lot of opinions on that. Our experts feel that reliability is in the range of 95 percent.

Senator **Glenn**. I have heard various reports and the figures were exactly that, a high of 95 and a low of 75.

Mr. **Snider**. That is the approximate range most often cited.

Senator Glenn. How do you take care of that now out at CIA or NSA where people may be completely aboveboard or legit, yet one-fourth could potentially have some problems?

Mr. Snider. We take a number of precautions.

First of all, if there is discrepancy shown on a particular question and it can't be resolved between one operator and the subject, we would give him a second examination by a different examiner to try to resolve any source of discrepancy on the chart.

I think more importantly than that, we simply will not take action based solely on the results of the polygraph examination.

Senator Glenn. There are some people who are just polygraph prone or polygraph vulnerable, or whatever you say, that it just gets to them. I have heard that.

There are people who are congenital liars, whose blood pressure is not disturbed one wit by lying. So, they get by.

Mr. Snider. I am not an expert on the subject, but I have seen how they do it at NSA.

What the process is intended to do is to establish a baseline of physiological reactions so if you are in an excited state, it will essentially form a baseline of your physiological reaction at that level of tension, so that when they get to the questions that are of interest on the exams, it measures the reactions above that established baseline.

So that if you are particularly nervous, your reactions would already be factored into the process. Reactions above that are what the polygraph measures.

Senator Glenn. How do you make certain that the polygraph record is kept secret?

I presume you get into personal questions, things like that, that could be damaging to a person if it were let out.

Are these kept very close?

Mr. Snider. Yes, sir. We only use personal questions with regard to employment at NSA. In the test program we do not ask personal questions.

Even with regard to the test program and the NSA, the polygraph results are kept within the office that administers them. They are not disseminated any further.

Senator Glenn. Do you think if we put in a system like this, that it should be strictly prospective or should it apply to everyone?

Should it apply to new employees who are coming in and they know it is part of their employment procedure or should it be applied to everyone?

What does the law say? Is there any constitutional problem?

Mr. Snider. There is no law per se regarding the polygraph. We have this limitation, of course, in our authorization bill in terms of the test program that we are authorized to run and do no more.

There are no statutory prohibitions on polygraph examinations per se that I am aware of.

Senator Glenn. Are there any States that admit polygraph evidence in court?

Mr. Snider. There are some States that admit such evidence based on stipulations. I know that there are quite a few, but I don't know how many. It is on stipulation of both parties that they admit results of the polygraph.

Senator **Glenn**. I am just concerned. I am not against this. I know CIA and NSA have used it and used it effectively. But people there know if they are going to apply for a job at CIA or NSA that they are going to go through a polygraph.

That is a bit different than taking people who have worked 25 years in the Pentagon, and saying, now you have to take a polygraph. I can see people getting nervous because they don't know anything about it. They have heard it is unreliable and heard this and heard that. It may be a different ball game.

Mr. **Snider**. You are quite right. It is a problem with our employees, no question about it, who have had access, who are offended by the idea that we are calling their trustworthiness into question.

Senator **Glenn**. You think it has been helpful?

Mr. **Snider**. Notwithstanding the problems it generates, yes, sir. I think definitely it ought to be part of the defense program.

Senator **Glenn**. Now, let me carry that a step further, too, because what I am about to say will be very controversial.

There are a lot of secrets over in the Pentagon, lots of secrets in NSA and CIA, lots of secrets in the contractors downhill. But there is one place that all that comes together and is reported to and people who have secrets are right here on the Hill.

Would you recommend that as part of covering this whole process and making sure that our whole process is covered, that any committee here on Capitol Hill that has oversight functions over the Pentagon or any of the contractors in any way whatsoever that deal with classified material also be subject to polygraph?

Senator **Wilson**. That will cut down on the number of applicants for the Intelligence Committee and the Armed Services Committee.

Senator **Glenn**. I am not talking only about the Intelligence Committee, but also the Armed Services Committee, the Foreign Relations Committee, and anyone who has oversight over a function of Government who would be required by the executive branch to get polygraphed as a result of this.

Would the Oversight Committee also be required because that is just as vulnerable a point as anywhere else in the chain to me?

Mr. **Snider**. I would have to give you a personal opinion on that one because I don't think the Department has faced that issue.

Yes, I don't see why you would want to make a distinction.

Senator **Glenn**. I don't either.

Mr. **Snider**. DOD clears, in fact, congressional staff for access to its information.

Senator **Glenn**. I would say we run our own polygraph operation here. That is one place I would vary, I guess, because I wouldn't want to see this used as a political thing. If people up here or in the executive branch do not like something, there would be all sorts of allegations back and forth.

I think we ought to run our own polygraph operation here. If we are going to require it of other folks and we are getting the same information here and we have staffs and people here just as they do in the Pentagon and contractors, it seems to me we should have the polygraph extended to Capitol Hill also if we are going to cover the whole operation as a Government.

I would want to keep the politics out of it. I would rather see us do our own polygraph operation right here and not depend on the Pentagon or someone else to do it for us.

Mr. **Snider**. I checked this before I left. We had DOD granted clearances of over 1,600 congressional employees and staffs. I was surprised to hear that large a number.

Senator **Glenn**. 1,600 just on the Hill?

Mr. **Snider**. 1,600, just the DOD clearance.

Senator **Glenn**. I am into my 11th year here. One of the things I was most surprised about when I came to Capitol Hill and went on the committee here was how classified material was treated.

I had just come out of 23 years in the Marine Corps and you talk about a way to ruin a career—let a piece of classified material get out.

I drove all night one night from Patuxent River, MD, because they had found a piece of confidential material—confidential means it is cleared for the front page of the Washington Post these days—but just confidential. It had been picked up on my desk up here and I was being written up.

That would have ruined my career in the Marine Corps or I would not have been promoted. I drove all the way from Patuxent River and sat in the BuAir building—it used to be on the site where the Vietnam Memorial is here, that old tempo that used to sit along the Reflecting Pool back there—and talked the duty officer out of writing that up officially on me.

That is the way it used to be treated. To come here on Capitol Hill and see secret material floating around and passed out with no marks on it at committee meetings shocked my soul when I got here. I have become hardened to it through the years.

I think if we are going to require polygraphing at other places, we are part of that defense chain right here, a key part. We are where all the information comes to right here. So, if there is one spot that is vulnerable in addition to DOD, it is us.

I will probably, at an appropriate time when we get ready to markup, either here or in full committee, put that in. If we are going to cover that operation across the river, we had better cover our operation here, too.

Thank you.

Senator **Wilson**. Thank you, Senator Glenn.

Senator Gramm.

Senator **Gramm**. Thank you, Mr. Chairman.

Let me go back to a question that was asked by the Senator from New Mexico because either I don't understand the facts or else you did not portray them.

You were asked the question what the constraint was in the use of polygraphs and the question ended up being expressed that in fact you placed no limits except the number of personnel.

Is that right?

Mr. **Snider**. I didn't explain that very well, Senator. We, obviously, have a limitation in the fiscal year 1985 Defense Authorization Act that says we cannot undertake any polygraphs apart from this 3,500.

Senator GRAMM. The fact is if you had a million operators who were capable of doing it under the restrictions imposed by the Congress, you could only do a 3,500-test program; is that right?

Mr. SNIDER. That is correct.

Senator GRAMM. Did DOD ask for 10,000 as a buildup, as a long-term equilibrium point and the Congress turned that down?

Mr. SNIDER. We were asked in previous hearings, Senator, what we thought would be a credible program, and we responded we would like to do 10,000 examinations a year, yes, sir.

Senator GRAMM. First of all, the figure was raised that if in the long-term equilibrium you decided to have everybody with compartmentalized clearance be given a test, how many people would it take to do that?

If you gave them a test every year, it would take 500 people.

The point was also made maybe we are going to do too much checking on too many people. The whole point in this bill is to mandate the reduction in the number of clearances. Whether you would want 500 or more to do it every year, or whether you would want the number of people you have in it, what we are looking at is an upper limit of 500.

I have to admit, and please forgive me for my strong opinion, based on relatively little information, but I am in the business where people form those opinions, the idea that we cannot expand the number of people who give polygraphs as rapidly as we expand the number of people who conduct brain surgery is just an insult to my intelligence. I don't believe that.

Let me ask you a question.

If I went over today, following Senator Glenn's suggestion, and I say, boys, give me a test and ask me the simple questions, how long would it take you to give me that test?

Mr. DONNELLY. About an hour.

Senator GRAMM. You are telling me that you could give me that test in an hour and yet an operator can only give 250 tests a year?

They must have one hell of a union.

Can you explain to me why they can only give 250 tests a year if they can give me a test in an hour?

Mr. DONNELLY. We really don't have any experience with regard to the counterintelligence test to really give you solid numbers. The 250 tests is based upon the productivity of our criminal polygraph operators. They are located in limited numbers, they do an awful lot of traveling.

Senator GRAMM. Let me stop you there because I have a limited amount of time.

You are telling me a lot of their time is spent traveling to give these tests?

Mr. DONNELLY. They feel they can just about run three of the criminal on the polygraph today.

Senator GRAMM. You gave me the figure of 250. Let me make my point.

If you have a scarce resource, you let the mountain come to Mohammed, not the other way around. If you were practicing medicine and you were going to go out and visit patients, you would treat a lot fewer people.

Since we have all these people with all these clearances, it seems to me one thing we could do is to bring them to the people doing the test, line them up at the door, have them come in and take the test. By simply changing the parameters of your test, I could increase your productivity fivefold or tenfold very easily.

Senator GLENN. Will you yield?

Senator GRAMM. I will be happy to yield.

Senator GLENN. Have you taken the test at NSA?

Mr. SNIDER. I haven't taken it personally.

Senator GLENN. I had some friends at CIA and I think it takes the better part of a half day to go through it. That is my impression anyway.

Senator WILSON. That is the lifestyle exam.

Senator GRAMM. I think that is a different kind of test than what we are talking about here.

Was Walker ever given a polygraph test?

Mr. SNIDER. Not to my knowledge.

Senator GRAMM. Am I correct or not from my knowledge of counterintelligence work in asserting that the Soviets direct their people not to put themselves in a position where they would be given a test or might be given a test?

Mr. SNIDER. We have heard that from several defectors, in fact.

Senator GRAMM. It seems to me that one of the strengths of the approach that we have taken in this bill is that, No. 1, by reducing the number of top secret clearances substantially, setting up an expectation that at some point during your career, and, quite frankly, I think Senator Cohen's proposal that at least you face an exit test, even though you might not be tested for 15 years, again one of the things we are trying to do is to get some deterrent out there.

In the situation of Walker we are not going to ask him, are you a good American, do you love the flag kind of stuff, do you like baseball, peanuts, and hot dogs. He passed that test.

The main truth is that in all probability he would have failed the simple question, "Are you a spy for the Soviet Union?"

He might well, had he known 15 years ago that he might be given this test at any point during his career or had he known the probability he would have been given it was five out of a hundred, he might well have not accepted the offer or sought out the offer to engage in spying against the Nation.

Just concluding, Mr. Chairman, No. 1, I reject the idea that an operator can only give 250 tests.

No. 2, I reject the idea that we can't come up with a more efficient training program. I cannot believe that if we can train brain surgeons more rapidly than this, that we cannot train people to give these tests.

I can't believe that if brain surgeons can do 500 operations a year, that we can only do 250 tests.

I would be willing to wager you I could take your best instructor, put him on television, set up 50 classes, give those classes to competent persons and increase the number of people turned out to pass your competency tests by a twentyfold margin.

It seems to me it is the kind of approach we had at the beginning of World War II. Had we done an interview before the Japanese bombed Pearl Harbor, hell, we lost the war. The truth was when we had to do it, we did it.

The final point I would like to make is that this bill specifically recognizes that we are not going to use the test as the only vehicle. It may well be, quite frankly, the problem is big enough that we can't have everybody have a Cadillac operator. We may have to produce a Chevrolet. Only in the case when we have problems with the Chevrolet do we bump somebody up to the Cadillac operator.

I think we have a real problem. I go back to my conclusion to the point that we are just at the tip of the iceberg in this new technology that we have invested billions of dollars in, coming on the production line.

If the Soviets can buy it for millions of dollars, then we are going to lose a tremendous investment that we have made and what that means is that you people are going to have to do a lot better job.

All I want to do is give you the tool.

Thank you, Mr. Chairman.

Senator **Wilson**. Thank you very much, Senator Gramm.

Senator Denton.

Senator **Denton**. Thank you, Mr. Chairman.

Gentlemen, it is my tendency in matters of detail that involve a couple hundred years of practice, to let the Department of Defense or the U.S. Navy, or whomever, work out the details of a general directive such as we say. I am sure that you will agree with us that there is too much classification.

If it were my prerogative, I would say, OK, guys, I want you to work out the classification problem. Over the next year show me, or suggest to me, a percentage of improvement that you can achieve in the various test scores, taking into account the number of people cleared.

I would say you take our directive, and reduce the numbers of people cleared, because that is entirely within your prerogative, not ours.

Like Senator Gramm said, I would like to provide you with the tools to do the job. But I don't want to provide you with tools that don't work, because I think that you guys know how to do your business better than we do, just as we know how to do ours better than you can tell us how to do it.

I want you to tell us whether or not you agree with what I have said when I finish.

I agree that there is overclassification, and I understand the Members' amazement about it. I think you have agreed that there is overclassification, too. There are too many people cleared, I agree with that.

I do believe that there is an amount of emphasis which would have a desirable effect on the problem, which is why the chairman has called this meeting. I admire this chairman, not only for conducting this hearing, but also for his rationalizations, and votes, and speeches on the floor.

Senator **Wilson**. I will extend your time. Thank you, Senator.

Senator **Denton**. I would rank them this way. With the observation we have had very few spies in the commissioned services of the U.S. Armed Forces. I am not positive, but this is the first time that I can remember in the U.S. Navy, in my lifetime, a convicted spy.

So, having said that, I would think that this man would have been deterred had we had a death penalty for his offense, which we are all in agreement should take place. I think that should be the number one objective, to take care of the odd freak who comes along who may either be persuaded, or persuade himself, to become a spy.

I hope we do find a way to do that. The only question I have is do we really want to have a mandatory death penalty for espionage if the espionage results in no major harm to U.S. security?

I think we ought to give some thought to that question. Did the accused, in his espionage, reveal confidential, top secret, or some code word information? Did it do severe damage? Or do we say anybody who does that should be killed?

We want to be sure of what we are doing before we pass that provision.

I would say the second policy that would have the most effect would be the polygraph test. The Secretary of the Navy believes, and I concur, that if we could have unrestricted use of polygraphs, with provisions to allay the proper concerns of the civil rights community, it would be an exceptional way to deter espionage. The polygraph questions could be reserved to such matters as, "Are you spying? Do you plan to spy?"

In other words, not ask, "Whom did you go out with last night?" or "Did you cheat on your income taxes last year?" That sort of thing.

Last, should there not be, while we are looking at this, a look at least at the Congress and staff of the Congress? To me I have seen fantastic leaks from within the administration, from within the legislative branch, which, to me, defy imagination. Those are the people who are supposed to be writing law and interested in keeping it.

There is an example of a man who was accused of trying to sell a top secret piece of paper to a country, offering it without selling it, and it turns out in the investigation that he had a top secret clearance, but he never had a background investigation at all.

The case was pretty much hushed up in the Justice Department. I am not going to offer a name, but that might not be a terribly isolated situation.

In other words, there are leaks from within the Senate, the House, by Senators, and by Congressmen. Not many, I hope, but some. Leaks by staffs are reasonably frequent.

Should we not take a look at what we are going to do about that?

There are amenities in the law in which a Senator or Congressman can, in pursuit of his duties, which is not an exclusively definitive phrase, give out information which is classified. Congressmen are not required to be automatically cleared for their job.

Overclassification does exist. The number of people who hold security clearances should be fixed, but I would rather leave it up to you as to how to do it, with some kind of congressional guideline. You need to suggest to us what is reasonable in the way of reducing them in terms of numbers.

On the polygraph, I would suggest to the chairman and our committee that we think about at least considering no restrictions, except that the questions be confined to matters that relate to security and activities of that person. I also believe that the death penalty certainly be invoked, but again, we want to give some thought to how many cases and to what kinds of cases.

Lastly, I would like to ask the gentlemen about the leaks with respect to Congress and the administration. Do you disagree with what I have said?

Mr. SNIDER. I don't find anything to disagree with, Senator. Some will be handled, of course, in different ways.

Senator DENTON. Senator Gramm informs me that the bill does not disagree with any of that. I thought the bill, however, stipulated some things for which you have asked an alternative approach, coupled with a little less specific guidance.

Is that incorrect?

Mr. SNIDER. That is correct. We would like to have more discretion in terms of where the polygraph would be used. We want the authority to use it.

Senator DENTON. Thank you, Mr. Chairman.

Senator WILSON. Thank you very much.

Senator Exon.

Senator EXON. Mr. Chairman, thank you very much.

I understand Senator Glenn raised the matter of giving polygraph tests to Members of the U.S. Senate and their staff. I understand that you agreed with him that this was a sound idea.

Is that right?

Mr. SNIDER. I don't recall his question being posed in terms of Members.

Senator GLENN. He gave a personal opinion. I did not necessarily exclude Members.

Senator EXON. Let me tie it down to Members of the U.S. Senate and our staff. We work very closely together.

What is your opinion on giving Senators and their staff polygraph exams Mr. Snider?

Mr. SNIDER. I expressed the opinion, a personal opinion, to Senator Glenn that I didn't see any reason to distinguish between congressional staffs who had access to the same sensitive information that we would require a polygraph for.

Senator GLENN. We were talking primarily about staff.

Mr. SNIDER. Again, that is not a departmental or administration view as far as I know.

Senator EXON. Let me say, speaking for one Member of the U.S. Senate, I have no objection whatsoever to taking a polygraph.

I think if it is true that proper intelligent use of polygraph is in order to try to close leaks. As a Member of the U.S. Senate, and this committee in particular, I have a lot of top secret information available to me and I would have no qualms whatsoever about subjecting myself to a polygraph. What is good for the goose it seems to me is good for the gander.

While it is well to think that the leaks we are concerned with came from other sources, and I suspect that they do, I believe that if we as Members of the U.S. Senate are going to suggest that polygraphs be used discreetly and intelligently, then we should agree to also submit ourselves to them. In other words, we should not be in a separate class from anyone else.

I suspect that sometimes some information of a highly secretive nature may leak out even when we don't intend it to. I worry continually about the situation of open and closed hearings which we go through all the time in this committee.

Most of our sessions are closed and we talk quite freely. There have been times when I felt that something has been said in open session that should not have been said. But, in any event, I want to tell you again from the standpoint of one Senator, I would not have any objection to subject myself or members of my staff to polygraph examinations.

I have two quick questions, Mr. Chairman.

There was an article, Mr. Snider, recently in the Washington Post which stated that many of the security clearance investigators are considered to be unsophisticated and untrained.

It also stated many of them receive low pay and start out at the GS-5 level.

In your opinion, how accurate is this criticism?

Mr. SNIDER. Let me put it this way. Our investigators all have to be college graduates. That presumes some level of sophistication.

Beyond that they are all trained, have to go to training school. They serve in a probationary period. They do start off, as I recall that article, at the GS-5 level, but within 1 year they are promoted to GS-7 and next year to GS-9. Their progression is very rapid in terms of higher rank.

Senator EXON. So, you don't believe that the comparatively low salary of $14,000 for a college graduate impedes your ability to select the right type of people for this program?

Mr. SNIDER. No, Senator, I don't. We have, in fact, a waiting list of people. We can be very selective in terms of whom we hire for investigators. The ones I have met are very sophisticated, very bright.

Senator EXON. I am surprised to hear that, but I take your word for it. If that is not an impediment, then we don't have to worry about it.

With regard to reducing the number of security clearances is it your opinion that it would be better to do an across-the-board reduction of all categories of individuals or is it better to concentrate on certain groups, say contractors, lower ranks, lower pay rates, and so on?

Mr. SNIDER. I think I would answer the question by saying probably some of both would be in order. We may want to use some of our examiners to polygraph particular groups who have access to highly sensitive information, to polygraph everyone in that group.

On the other hand, we may want to take some of our resources and say that everyone with top secret clearance or secret clearance in fact could be subject to a polygraph during their careers. We may want to use the limited examiners we have, to conduct such polygraphs on a random basis, so that we would get deterrence within a larger population.

This is the reason I was recommending in our statement that we have the discretion to decide these kinds of questions ourselves.

I think it is a mistake to try to write a statute that sets out how we are going to do the polygraph because I think there is a lot of judgment to be applied to it, given our limited resources.

Senator EXON. In your experience are leaks as serious a problem as espionage?

How serious are unintentional and undesigned exposure of information such as someone with top secret clearance telling something to the spouse or to a father or son or brother or sister?

Mr. SNIDER. I am sure that happens quite frequently. Telling your wife or husband something you were not supposed to say. I am sure anyone who has worked in the classified area over a long period of time has had that experience.

How much of a problem is it? I don't think in general that it is much of a problem. Generally the information doesn't go beyond the wife or relative.

Senator EXON. In other words, if you tell your wife, she might not recognize it as such or doesn't think it is that important?

Mr. SNIDER. I am not suggesting we condone it, but we recognize it happens.

Senator EXON. Thank you. That answers my question.

Thank you, Mr. Chairman.

Senator WILSON. Senator Glenn.

Senator GLENN. Just a brief comment and a question on another matter here.

As far as Senator Gramm's comment on training of operators, I am sorry he left, but I think we have this 3,500 test now. We may be strapped a bit on operators now to expand this thing tremendously.

I think what Senator Exon just mentioned and asked you about the GS rating, and so on, if this were a real career path and people saw this as a service that was going to be required through the years, they would train for that like they train for court reporter, or whatever.

It is a career track and people are proud to get into it and proud to serve. They expect to be promoted in time and it is not something that is fly-by-night and we have a polygraph now and not later. It is not an attractive thing to go into right now.

If it were a career path and required on a large scale, I have no doubt the trained people would be there. We could take care of that without any problem. I don't agree with his fears about being unable to train this whole group of people we need.

Senator Gramm asked whether the Soviets told their people to avoid situations where they could be polygraphed. I believe you answered yes.

Mr. SNIDER. We have had several instances where we know that to be a fact.

Senator GLENN. Christoper Boyce, on the other side of this, who was convicted for espionage on behalf of the Soviets, told the Permanent Subcommittee on Investigations over in the Governmental Affairs Committee of which I am a member, that the Soviets tried to get him to apply for employment at CIA or State. Boyce refused because, just as you say, he was afraid he could not pass the polygraph, but the Soviets told him not to worry because, "We can train you to beat them."

Is that possible and if we put this into effect here, are we going to windup with training courses on how to beat your friendly polygraph advertised in the Washington Post?

Can you train a person to beat a polygraph?

Mr. **Snider**. I will ask Jack to answer that.

Mr. **Donnelly**. They have said that to a number.

Senator **Glenn**. You mean they told Boyce that?

Mr. **Donnelly**. Boyce said they told him they would train him to beat the polygraph, but they didn't give him that training. We have heard them make similar remarks to a number of other people in our counterintelligence operations.

So far they have never given that training to anyone. So, we are not sure they can do it. We are alert to it and we are trying to find out if they do do it.

Senator **Glenn**. Let me turn this around a moment and you may not want to answer this question. If you don't, say so.

Do we train our people to beat other people's polygraph tests?

Mr. **Donnelly**. No, we do not.

Senator **Glenn**. In other words, we know of no way you can train a person to beat a polygraph; is that correct?

Mr. **Donnelly**. To the best of my knowledge, that is correct, not in the United States.

Behind the curtain, in Czechoslovakia there is one written about in the newspapers and magazine articles, for that purpose. There is some doubt as to the viability of that training, whether it really works.

Mr. **Snider**. There may be things we don't know about that other agencies do so I am somewhat leery of giving you an absolute, "We don't do it."

Senator **Glenn**. I understand. What you don't feel comfortable with, I want you to say so. We may ask some other folks on that.

Thank you, Mr. Chairman.

Senator **Wilson**. Thank you very much, gentlemen.

We do have a second witness. We will excuse you with thanks. We may wish to contact you further.

Mr. **Snider**. Thank you, Senator. It is our pleasure.

Senator **Wilson**. Thank you very much for your contribution.

Our next witness is Hon. Chapman B. Cox, General Counsel of the Department of Defense.

Welcome, sir. Sorry that we have taken your afternoon.

STATEMENT OF HON. CHAPMAN B. COX, GENERAL COUNSEL, DEPARTMENT OF DEFENSE

Mr. **Cox**. That is all right. It is for a good cause, sir.

Good afternoon, gentlemen. It is a pleasure to be with you, Mr. Chairman.

With your permission, I would like to first submit my formal statement for the record.

Senator **Wilson**. We will enter your statement into the record in its entirety.

Mr. **Cox**. Before proceeding with your questions, I would like, with your permission, to briefly summarize the Department's position with respect to proposed changes to the Uniform Code of Military Justice relating to espionage offenses.

First, a brief word about the current law.

The Uniform Code does not currently contain an offense for peacetime espionage. There are wartime espionage offenses in the code and there are lesser peacetime offenses related to espionage; for example, unauthorized disclosure of classified information. But there is no peacetime espionage offense.

Certainly we would prefer to have a peacetime espionage offense in the Uniform Code and would have preferred to for some time. Having the option of prosecuting military offenders in a military court provides important advantages to protect the Government's interest and enhances the administration of justice.

These include flexibility in choosing the appropriate forum for trial, the opportunity to give greater protection to sensitive information used as evidence, inclusion of lesser included offenses under the Uniform Code which might not be offenses under the civilian criminal statute, and finally, an adequate range of punishments commensurate with the seriousness of the crime.

With all these advantages to having a military peacetime espionage offense, why haven't we pressed for such a provision in the past?

Well, traditionally, although we would have preferred to have a peacetime espionage military offense, we believed that the interests of the Government and of criminal justice were adequately served by relying on civil authorities to prosecute peacetime espionage committed by service personnel.

However, recent developments have caused us to reevaluate our position in this regard. These developments are:

First, in recent years many have become concerned about the death penalty provisions of the civilian espionage statute and whether or not they were constitutionally valid. This growing concern was confirmed in 1984 by the Ninth Circuit Supreme Court in its decision in the *Harper* case when it struck down the death penalty in the civilian statute.

A second recent development is that we have had growing concern about the sensitivity of evidence in these kinds of cases and our ability to protect that sensitive evidence from disclosure.

A third development is a general desire with respect to the total criminal system that we would have increased integrated deterrent effect in this area of espionage. In other words, that we could combine the different incentives and disincentives of both the military and civilian criminal statutes to their maximum advantage.

Finally, over the past, say, 5 to 10 years, there has been an increased frequency of espionage cases where the disparity of punishment between that would be available under the military code and what would be available under the civil code for the same offense has been a significant factor.

So, with all of these increased concerns, we do believe that we need to improve the law.

Now, the question is how can we improve the current law?

First, we believe that we can correct the disparity between the military and the civilian codes by adding an espionage offense to the Uniform Code of Military Justice which is similar to the civilian espionage offense and it should not be limited either to wartime or to peacetime.

It should be an espionage offense just like the civilian offense that is equally applicable under any condition.

Second, we believe that we should provide constitutionally valid capital punishment for espionage in both the military and the civilian code.

What are we doing about this?

We have developed proposed legislation to accomplish both of these objectives which is currently being coordinated in the executive branch. It would add a new Article 106a to the Uniform Code which mirrors the civilian Federal espionage statute.

It also provides the death penalty under a constitutionally valid sentencing procedure.

We also strongly support section 5 of the Gramm bill, subject to three minor changes which are noted in my formal statement and to one more significant change which we would urge.

We would prefer that the mandatory sentencing provisions of the Gramm bill be deleted in order to give the Government more flexibility in protecting its interests in these complex and sensitive cases and in order to insulate court members from focusing on the sentencing consequences when determining guilt.

This concludes a summary of my statement, sir.

I will be pleased to respond to your questions.

[The prepared statement of Mr. Cox follows:]

PREPARED STATEMENT OF CHAPMAN B. COX, GENERAL COUNSEL, DEPARTMENT OF DEFENSE

Mr. Chairman and Members of the subcommittee: I appreciate the opportunity to appear before you today to discuss the prosecution of espionage related-offenses under the Uniform Code of Military Justice (UCMJ). The Department of Defense is grateful for the efforts of the Subcommittee in calling attention to this important subject, and for your continuing interest in the military justice system.

I would like to begin by discussing the current statutory basis for prosecution of these offenses. Then I will describe some related problems which we identified and outline the approach we used to develop proposed solutions. Finally, I will comment on current legislative proposals, including the UCMJ amendment contained in S. 1301.

CURRENT LAW

Several articles of the UCMJ provide the primary grounds for prosecuting armed services personnel for espionage and related offenses. These provisions remained largely unchanged since enactment of the UCMJ in 1950.

Article 106, which is applicable "in time of war," proscribes the offense of "lurking as a spy or acting as a spy." The mandatory punishment for this offense is death. This is the only article of the UCMJ that carries a mandatory penalty.

Article 104 covers "aiding the enemy". This includes the offenses of "giving intelligence to the enemy" and "communicating with the enemy." The UCMJ permits the death penalty for these offenses.

Article 134, "the general article," permits incorporation of non-capital civilian offenses in the UCMJ. Under this provision, we may prosecute offenses such as 18 U.S.C. § 793 ("Gathering, transmitting, or losing defense information") and 18 U.S.C. § 798 ("disclosure of classified information"), each of which carries a maximum period of confinement of ten years. However, we can not prosecute the offense of espionage (18 U.S.C. § 794) under the general article because it is a capital offense.

Article 92 governs failure to obey orders or regulations and dereliction in the performance of duties. There are numerous rules covering access, handling, and disposition of classified information; other rules restrict contacts between service members and foreign governments. The maximum punishment for violation of these rules is dishonorable discharge, confinement for two years, and total forfeitures.

Because most espionage-related offenses constitute crimes under both federal civilian law and the UCMJ, service members accused of these offenses may be prosecuted by either the Department of Justice or the Department of Defense. There is a Memorandum of Understanding between the two Departments that requires consultation in the course of investigation and on the choice of forum. We have had excellent relations with the Department of Justice on these matters.

THE NEED FOR AN AMENDMENT TO THE UCMJ

The Department of Defense has established the Joint Service Committee on Military Justice, which is responsible for recommending changes in both the Uniform Code of Military Justice and the Manual for Courts-Martial. This Spring, we asked the Joint Service Committee to consider the need for amendments to the military laws related to espionage. The Joint Service Committee's task was based on two problem areas we identified in current law with respect to espionage offenses.

The first is disparity between military and civilian law with respect to punishment for peacetime espionage. There is no article of the UCMJ that expressly addresses peacetime espionage. The two articles of the UCMJ that address espionage-related offenses are wartime offenses. Article 106 applies only "in time of war." For purposes of military law, "time of war" means a war declared by Congress or a factual determination by the President that a "time of war" exists due to the existence of hostilities. Similarly, aiding the enemy under Article 104 applies only when an enemy can be identified based upon the existence of a declared war or other hostilities.

As noted above, the federal civilian offense of espionage cannot be incorporated in the UCMJ through the general article (Article 134), because it is a capital offense. Therefore, peacetime prosecution of espionage related offenses under the UCMJ is limited to lesser non-capital offenses which can be incorporated under the general article, such as transmitting defense information, or disclosure of classified information. However, these lesser offenses carry a maximum punishment of ten years confinement, while the federal civilian offense of peacetime espionage carries a maximum punishment of life imprisonment.

It is our position that any legislation in this area should be directed toward eliminating the disparity between the 10 year maximum period of confinement available under military law and the opportunity to obtain a sentence to life imprisonment under federal civilian law.

We have also considered the issue of capital punishment for peacetime espionage. The Ninth Circuit, in *United States* v. *Harper*, 729 F.2d 1216 (9th Cir. 1984) held that the procedures for imposing the death penalty under 18 U.S.C. § 794 did not meet the constitutional requirements established by the Supreme Court for capital cases. The Senate, in the last Congress approved legislation to establish valid death penalty procedures for section 794, but the House did not act prior to adjournment. The Administration has again requested approval of this legislation. We recommend that legislation authorizing the death penalty for similar espionage offenses be enacted as part of the UCMJ.

The second problem we have identified relates to the maximum punishment for wartime offenses. The offenses of spying under Article 106 and aiding the enemy under Article 104 both require proof that the information was provided to the enemy or was gathered with the intent of aiding the enemy. These statutes do not cover unauthorized transmission of defense information to a foreign government in wartime where it cannot be proved that the information was provided to the enemy or was gathered for the purpose of aiding the enemy. As a result, the maximum punishment that could be obtained in such a case through incorporation of 18 U.S.C. § 793 would be ten years confinement.

This is in contrast to federal civilian law in 18 U.S.C. § 794 which proscribes gathering or delivering defense information to a foreign government "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation. . . ." Because this capital offense cannot be incorporated into the military justice system through Article 134, there is a need for a separate article of the UCMJ to eliminate the disparity between the 10 year maximum period of confinement available under military law and the maximum of life imprisonment under federal civilian law. Such a statute also should permit imposition of the death penalty.

PROPOSED LEGISLATION

As mentioned previously, the Joint Service Committee was tasked with drafting a proposed amendment to UCMJ to correct the problems we had identified in the espionage statutes. When recent events underscored these problems, we directed the Joint Service Committee to give priority attention to this matter. Our draft legislative proposal, which we are coordinating within the Executive Branch, is a result of the efforts of the Joint Service Committee. The proposed legislation mirrors the provisions of the federal civilian espionage statutes (18 U.S.C. § 794) in a new Article 106a.

Section 5 of S. 1301 would also create a new Article 106a in the UCMJ, which would proscribe communication, delivery, or transmission of defense information to a foreign government or to other specified foreign entities "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation." This amendment generally is patterned after 18 U.S.C. § 794, with several differences. The Department of Defense strongly supports the objectives and general provisions of this portion of S. 1301, subject to the following recommendations:

The phrase "in time of peace" should be deleted from the title. As noted above, there is a need for an espionage statute in time of war to supplement the present Articles on spying and aiding the enemy to address situations in which information is provided to a nation that is not legally an "enemy" engaged in hostilities with the United States.

The phrase "at any time" should be deleted. All offenses under the UCMJ apply in both peacetime or war unless expressly limited.

The phrase "shall be punished by death or by imprisonment for any term of years or for life" does not reflect the terminology used in the UCMJ. We recommend: "shall be punished by death or by such other punishment as a court-martial may direct," the phrasing that is used elsewhere in the UCMJ.

S. 1301 provides for death or mandatory life imprisonment in the event that the information is provided to the Government of the Soviet Union or another communist country. We agree that the transmission of information to these nations would constitute a very serious offense. However, we recommend against the mandatory life imprisonment provision for two reasons.

First, there is the issue of damage limitation. Frequently, in an espionage situation, an investigation may reveal only the tip of the iceberg. There is a need to assess damage, and to probe deeper for other offenders. With a mandatory life imprisonment provision, the government is limited in its ability to obtain information from the accused. I wish to emphasize that this does not mean that the government would not take seriously the need for strong punishment in such cases; but we should not create rules that so rigidly limit the government's flexibility.

Second, a mandatory life sentence provision paradoxically would reduce the likelihood of obtaining convictions in some cases by causing the court members to focus on sentence, rather than on the issue of guilt, during the findings stage of the trial. Experience in both civilian and military trials has demonstrated that when the jury focuses on the sentencing consequences of a mandatory punishment rather than on the issue of guilt or innocence, there is an increased likelihood of an acquittal despite evidence sufficient to support a conviction. Although all these cases are serious, some are less serious than others; and it would be most unfortunate to have acquittals in the less serious cases—which are still detrimental to our national security—because of a mandatory life sentence provision.

The creation of a new espionage offense in the UCMJ would represent an important addition to military law. We are grateful to the efforts of this Subcommittee in taking the lead on this vital issue.

With respect to the amendments to the Federal Criminal Code contained in S. 1301, we defer to the Department of Justice. We have been advised that the Department of Justice intends to comment on the Title 18 amendments proposed in S. 1301 in a report to this Committee.

Mr. Chairman, this concludes my prepared statement. I would be pleased to respond to your questions.

Senator WILSON. Thank you very much, Mr. Cox.

We appreciate your written statement and the clarity with which you have summarized it.

Mr. Cox, the Uniform Code of Military Justice was enacted 35 years ago last month. It has never contained the so-called peacetime espionage article. To my knowledge, during the 35-year period the Department has not proposed that such an article be included in the UCMJ. The Department now supports the addition of an article proscribing such conduct and providing a death sentence for it.

A couple of questions.

First, I gather from your testimony that you feel there has been a need, not a change in circumstances, which now dictates that an article be included.

Mr. Cox. There has been a growing discrepancy between civilian and military code provisions on espionage over the years. Those concerns have blossomed as a result of recent events that have emerged.

We had, for example, our Joint Service Committee that deals with recommending changes to the Uniform Code already working on this issue when the *Walker* cases occurred. So, it is not just the *Walker* cases.

The *Harper* case was decided in 1984. It confirmed that the capital punishment in the civilian code was unconstitutional, at least the way the penalty was imposed under that specific provision.

There was concern prior to 1984, in fact public testimony by the Justice Department that this might not be a constitutionally valid provision. So, these concerns have grown over the years.

Since 1975, I think, we have had something like five trials under civilian statutes where life imprisonment was imposed.

Now, if the conditions under which those offenses occured would have been better tried in military courts, we would not have been able to try them under the UCMJ and obtain life imprisonment even, let alone the death penalty, because we would have had a 10-year maximum punishment, as explained in my formal statement.

So, these kinds of developments have been occurring to the point where, as I mentioned, we believe we need to bring the military code into parity, if you will, with the civilian code to maximize our ability to deal with these offenses and to promote the ends of justice as well as protecting the interest of the Government.

Senator WILSON. Would it be a fair statement that in that 35-year period there did not appear to the armed services to be a serious peacetime espionage problem in terms of espionage committed by members of the armed services, while at the same time there appeared to be a judicial anathema to the death penalty throughout the country in terms of civilian cases and for that reason nothing happened?

Mr. Cox. I would agree with Senator Denton that there have not been very many military espionage problems. But even one is too many.

It is incumbent upon us to have a code which permits us to deal with those problems when they arise. In the past, as I mentioned, we have taken the position that the interests of the Government and the administration of justice were adequately served by prosecution by civilian authorities.

But all these other events over the last 10 years have caused us to reevaluate that.

Senator WILSON. I think in the interest of time we should stipulate that one case of espionage is too many and the problem certainly exists and some problems have manifested themselves.

Let us talk about your concern with respect to the mandatory nature of the death penalty prescribed by S. 1301. In your statement you mentioned two possible drawbacks to the mandatory death or life imprisonment provision contained in article 6(a).

You indicated that these provisions might limit the ability of Government to bargain with an accused and thereby limit damage. You also expressed concern that some prosecutions might be lost because court members would focus on the mandatory punishment during the phase of the trial concerning guilt or innocence.

Of the two concerns you raise, I think that the former is perhaps the more significant. I would think that since we are talking about a general courts martial where the jury are military personnel, they would be less likely to focus on the sentence, but you raise an interesting point at the very least.

My concern is that you may not have the same kind of flexibility that civilian prosecutors do in terms of the plea bargain they engage in in order to secure, for example, in organized crime cases, the testimony of someone who is really an underling in order to gain evidence against those who are really directing a corporate crime.

In this sense, to draw the parallel, do you think you would lose the flexibility that might otherwise prompt the accused to become a witness or at least furnish information that would implicate his superiors?

Mr. Cox. Yes, that is a good summary of the concern. I agree with you, of the two concerns raised in my statement, the first is certainly the most serious.

In these kinds of cases you frequently get involved in a very difficult balancing function where you are balancing the interests of criminal justice, on the one hand, against the interests of our national security.

The prosecutors and representatives of the Government in that case are faced with a very difficult dilemma in trying to assess the damage that the offense has caused to the national security while at the same time trying to prosecute a suspected offender.

If the criminal statute imposes upon them certain disincentives to their bargaining with the offender to get information from him, it makes that balancing all the more difficult and creates a certain inflexibility which either damages the national interest, on the one hand—where you say, "in the interest of the criminal justice we have to forego our right to get information and go ahead and prosecute"—or, on the other hand, in the interest of national security you say "forego the prosecution."

Any inflexibility in that increases the difficulty of the very delicate balancing that prosecuters have to do.

Senator WILSON. Thank you. My time has expired. I will have additional questions on the proposed article 106(a) and also questions relative to the procedure prescribed to cure the defects cited in *United States* v. *Manson* with regard to procedural problems raised by capital punishment.

I will submit those for the record.

Mr. Cox. We will be happy to answer them for the record, sir.

Senator WILSON. Thank you.

Senator Glenn.

Senator GLENN. Thank you, Mr. Chairman.

I have been a bit concerned about the breadth of this thing. I guess the wording could be considered imprecise. Perhaps it could be interpreted very, very broadly.

For instance, and I won't read the entire section on page 3 of the print of the bill, it basically says any person who delivers, communicates or transmits to any foreign Government any document or information relating to the national defense, or information relating to the national defense, shall be tried and shall be punished by death, and so on.

In a Communist country, he shall be punished by death. The term, "Or information relating to the national defense," is very broad.

Don't you think our people would probably like to have a phone directory of the Soviet Defense Ministry and vice versa?

It is related to the national defense.

Mr. Cox. Yes, you have to read the rest of the language of the statute. It talks about for the purpose of harming our interests or aiding their interests.

The broader answer to your question is that that language is the same language of the Federal civilian espionage statute. One of the reasons that we are promoting that language is there is a body of case law that goes with the interpretation of that language.

There are cases, for example, that stand for the very clear proposition both that the information must be nonpublic in nature and that it must be provided either to advantage a foreign country or with an intent to injure the United States.

Senator Glenn. The phone book wouldn't qualify?

Mr. Cox. No, because it is public information. It has to be nonpublic information and has to be provided with the requisite intent.

Senator Glenn. In amending the Uniform Code, UCMJ, this bill would create a criminal espionage offense punishable by death or life imprisonment "which shall be tried by a General Court Martial."

Does that language prevent the Justice Department from prosecuting a member of the armed services under the criminal espionage statute in title 18?

Mr. Cox. No, sir. Our Memorandum of Understanding with the Justice Department would not be affected by the statute. That means that it shall be tried by a general court-martial as opposed to a special or summary court.

It would not impact on our Memorandum of Understanding with Justice under which we in all of these sensitive cases coordinate with them and determine whether the forum to better try the case is a civilian Federal court or military court.

Senator Glenn. Has this been discussed with Justice?

Mr. Cox. Yes.

Senator Glenn. I believe they indicated unofficially they opposed this section because they were afraid it would remove that option for future prosecutions?

Mr. Cox. It is my understanding from our discussions that if we interpret it in that way and the report language indicates that, that they have no problem with it. It may be better to take it out.

We will be happy to work with you on making sure it is consistent with other code language which doesn't impact upon our Memorandum of Understanding.

Senator GLENN. Thank you, Mr. Chairman.

Senator WILSON. Thank you, Senator Glenn.

Senator Exon.

Senator EXON. I have a couple of short questions.

Mr. Cox, can you briefly explain to me in layman's language what punishment the law now provides for withholding knowledge of a spy?

For example, didn't Mrs. Walker know that her husband was a spy?

I assume that the statutes apply which would prevent her from testifying against her spouse. Is that correct?

While you are answering that question, please expand upon it. If an individual has firsthand knowledge that someone is a spy, what obligation does that individual have under the law to report it, if any?

Mr. COX. That is a very difficult question, sir. I cannot give you a reasoned answer off the top of my head. There are certain laws with respect to knowledge of serious felonies—of which espionage is one—that place an obligation upon the person who has the knowledge to come forward.

There are also certain privileges of certain people who have this knowledge to the effect that they are not encumbered with such obligation; for example, a lawyer who learns it in confidential communications.

Senator EXON. A lawyer?

Senator WILSON. I detect a bias.

Mr. COX. Sometimes spouses also have privilege against having to reveal the information. I am telling you off the top of my head. It is difficult to make these distinctions for you.

With respect to the spy, himself, I think the formulation I gave Senator Glenn is about as clear and concise in a short phrase as I could give it. That is that the spy must provide the information which is nonpublic in nature with the intent or the knowledge that it would give advantage to the foreign country or with the intent or knowledge that it would injure the United States.

Senator EXON. I assume you have studied the Gramm bill from a legal standpoint, haven't you?

Mr. COX. Yes.

Senator EXON. Is it true that the Gramm bill specifically addresses only espionage on behalf of a Communist nation? If it became law, would the penalty provided therein apply only to a Communist nation?

If that is so, it seems to me that the spying for a non-Communist nation is just as serious a threat to our national security as spying for a Communist nation.

Could you tell us the difference?

Mr. COX. The answer is no, it doesn't just apply to a Communist nation. It applies to any foreign government. The mandatory sentencing only applies to a Communist country. That provision we would recommend be deleted, the mandatory sentencing provision, for the reasons I stated to Senator Wilson.

Senator EXON. One last question.

Does the Department of Defense have an opinion on another bill in this area that I understand has been introduced or is going to be introduced which would mandate upon conviction not only the death penalty, but that the death penalty be shown on television?

Has the Department of Defense looked at that provision? What do you think of it?

Mr. COX. We have the same opinion on that, which is consistent with our earlier expression, that we would recommend against a mandatory death sentence.

Senator EXON. That is also your view on showing the carrying-out of the sentence on television?

Mr. COX. Yes, sir.

Senator EXON. Thank you, Mr. Chairman.

Senator WILSON. Thank you, Senator Exon.

The Chair is pleased to welcome and recognize our colleague, not a member of the subcommittee, but a member of the full Committee on Armed Services, Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

On the mandatory death penalty issue I have a number of questions. You have indicated that the Defense Department is opposed to the mandatory death penalty.

As I understand it, this bill would provide for either a mandatory life or mandatory death penalty. I presume that is the heart of this bill. There are two options, if I understood the circumstances, either a mandatory life sentence or a mandatory death penalty.

You are opposed to providing only those two options?

Mr. COX. Yes, sir.

Senator LEVIN. You are opposed to the heart of the bill as far as I am concerned. You would like to see an optional death penalty and an optional life imprisonment?

Mr. COX. We would like to have a maximum penalty of death and anything up to that.

Senator LEVIN. Being optional?

Mr. COX. Yes.

Senator LEVIN. If there is going to be a death penalty—I know you don't accept that position—if there were going to be a mandatory death penalty, would you support its being limited to the situation where the espionage benefits a Communist country?

Mr. COX. I think that is dangerous because you get into all kinds of situations of trying to figure out who our real adversaries are, No. 1.

No. 2, even if you assume that our real adversaries are Communist, there might be problems of proof during a trial as to whether or not there was a indirect link between the nation who got the information and the adversary, be it Communist or not.

So, the bill would have to be cleaned up to make sure we clarify those ambiguities if we do keep the mandatory death sentence. Otherwise it might be an unconstitutional provision; I don't know.

Senator LEVIN. We also have adversaries who are non-Communists.

Mr. COX. Yes, sir.

Senator Levin. Is it a rational distinction that you get mandatory death if the adversary is Communist, but not if the adversary is non-Communist?

Mr. Cox. I don't believe so.

Senator Levin. The bill amends title 18 in the Criminal Code as well as the Uniform Code of Military Justice?

Mr. Cox. Yes, sir.

Senator Levin. Are you prepared to comment on title 18 of the Criminal Code?

Mr. Cox. I would be happy to take your questions on that. The Department's position on title 18 is that we support the Thurmond bill. That is an administration bill. We think the Thurmond bill adequately covers the title 18 problem.

Senator Wilson. The Thurmond bill is S. 239, last year's S. 1765 which passed the Senate.

Mr. Cox. Yes, sir. Our proposal with respect to the Military Code, is in total concurrence with that approach.

Senator Levin. Because of the Executive order?

Mr. Cox. Yes, sir.

Senator Levin. Going back to title 18, you are saying that the Department of Defense opposes this provision in this bill relative to title 18; you favor a different approach which is the Thurmond bill?

Mr. Cox. I guess it is not entirely different. I think they are similar in their purpose and so I wouldn't say that I oppose Senator Gramm's bill.

I think Senator Gramm is trying to do the very same thing that Senator Thurmond is trying to do in a different way, but we support the way Senator Thurmond is trying to accomplish the goal.

Senator Levin. I am suggesting we support Senator Gramm; I am talking about the bill. To the extent his bill is inconsistent with the Thurmond bill, you would favor the Thurmond bill and not favor, by definition, the Gramm bill?

Mr. Cox. That is right.

Senator Levin. Has the reliance on the Executive order for a procedure for determining whether someone gets the death penalty or not been tested in court?

Mr. Cox. It has not been tested yet constitutionally. We have two cases in which the death penalty has been imposed under the new procedure and they are now working their way through the appellate system.

Senator Levin. Is there any reason why those provisions should not be incorporated, why the Thurmond provisions should not be incorporated in this bill relative to the Code of Military Justice as well as your preference for them relative to title 18?

I happen to oppose the death penalty, by the way. I hope I have not mislead anybody. I oppose it because you can't correct your mistakes, because we disproportionately impose it on people who are indigent, who can't afford the best lawyers, and for a lot of reasons.

But assuming we are going to do something like this, is there any reason why we should not incorporate the protection, to the extent there is protection in the Thurmond approach, in this bill rather than relying on the Executive order which is being tested in court?

Mr. Cox. We believe that the sentencing procedures provided by the Congress under the Uniform Code of Military Justice are the right ones for the military system. We believe it should be the President as Commander-in-Chief, who establishes the guidelines and procedures that meet the needs of the Armed Forces for sentencing in all of the military justice system.

We also believe that the Executive order meets all the constitutional requirements. In fact, if you lay them side by side with the Thurmond bill, they would be very similar. There would be some additional ones relating to the military system, but I think they are very similar.

Senator Levin. Didn't the Military Court of Appeals say that the requirements for invocation of the death penalty could be met by either Executive order or by the Congress?

That has not been determined? Did the Court of Military Appeals say that?

Mr. Cox. The Court of Military Appeals said that.

Senator Levin. You differ with that judgment?

Mr. Cox. No, sir.

Senator Levin. Is there any reason why the Congress can't incorporate these provisions?

Mr. Cox. Because we believe it is better for the President to have the flexibility to do it.

Senator Levin. You don't doubt we can legally do it?

Mr. Cox. You can do it legally either way.

The second reason besides the fact the President is the one that should do it, is that we now have this procedure in the manual with respect to all of our capital punishment. If you as a Congress impose the statutory system on one punitive article, you create doubt that the other procedure is constitutionally valid.

We would strongly urge you against doing that.

Senator Levin. Has the military justice system ever made a mistake in finding someone guilty of a capital offense?

Mr. Cox. Not to my knowledge.

Senator Levin. Has there ever been a mistake in the history of the military criminal justice system?

Mr. Cox. You said capital punishment?

Senator Levin. No, I didn't. I said capital offense.

Mr. Cox. I don't know on capital offense. To my knowledge, they have never made a mistake in imposing the death penalty.

Senator Levin. Could you find out what errors have existed in the military criminal justice system?

It is a lot purer than the civilian justice system if it has never made a mistake in a capital offense.

Mr. Cox. I will try to find out.

Senator Levin. Thank you.

Senator Wilson. Thank you, Senator Levin.

Mr. Cox, let me say one or two things before we excuse you.

First, I gather from your testimony that the Department is working on a bill.

Mr. Cox. Yes, sir. We finished our deliberations and our deliberative process just recently. I forwarded our Department bill to OMB today for the coordination process.

The Joint Service Committee had started working on this back in the spring and it was going on a regular schedule which we sped up about a month ago. I promised the Secretary a report on the 20th of June.

As a result of that, all these things are converging.

Senator Wilson. Your bill deals both with military and civilian espionage, wartime and peacetime?

Mr. Cox. Only military, sir.

Senator Wilson. Only military?

Mr. Cox. Yes, sir. The administration position on the civilian statue——

Senator Wilson [continuing]. Is in the Thurmond bill?

Mr. Cox. Yes, sir.

Senator Wilson. When you have received such clearance as required, the committee would obviously have a great interest in your draft legislation.

Mr. Cox. Yes, sir.

Senator Wilson. Can you give me some idea when we might expect it?

Mr. Cox. I can't tell you how fast the OBM process will work, but we have been working with the people on the staff and on Senator Gramm's staff. I don't think we are far apart. We will get it to you as soon as we possibly can.

Senator Wilson. We thank you very much, Mr. Cox.

The record will be kept open if there are questions from other members that they would like to submit to you for the record as well as to Mr. Snider.

[Questions with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR PETE WILSON

Senator Wilson. Mr. Cox, in October 1983, in the Army Courts-Martial case of *United States* v. *Matthews*, the United States Court of Military Appeals ruled the death penalty procedures then in effect under the UCMJ and the *Manual for Courts-Martial* did not satisfy the constitutional requirement that court members make specific findings of individualized aggravating factors. The court further said, in what may have been *dicta*, that either the Congress or the President could remedy that defect.

In January 1984, the President, through executive order, amended the Manual for Courts-Martial to provide for new death penalty sentencing procedures by courts-martial which were designed to satisfy the constitutional requirements for imposing of capital punishment.

I have a three part question in this regard.

First, does the Department believe that the President has sufficient statutory authority under Article 36 of the Uniform Code that he, through executive order, may prescribe constitutional procedures for imposition of capital punishment under the UCMJ, and that statute is not needed in this area?

Mr. Cox. The President's power to prescribe the Manual for Courts-Martial is derived from his constitutional authority as Commander-in-Chief, the rulemaking authority of Article 36, and the authority to establish limitations on punishments in Article 56. Congress has authorized the death penalty for specified offenses in the UCMJ. The President's rules meet all applicable standards for imposition of capital punishment.

Senator Wilson. Second, have the present death penalty procedures in the *Manual for Courts-Martial* been reviewed for constitutionality by any federal or military appellate court and does the Department believe those procedures meet all constitutional requirements?

Mr. Cox. Since the new capital punishment rules were issued in 1984, there have been two homicide cases in which the death penalty was adjudged. One case currently is pending before the Army Court of Military Review. The other case is awaiting action by the convening authority.

It would be inappropriate for me to comment on the two cases now under review. As a general matter, we are confident that the capital punishment rules in the Manual for Courts-Martial meet all applicable constitutional requirements.

Senator Wilson. Finally, if this subcommittee were to report a bill containing a capital offense peacetime espionage article such as the one contained in S. 1301, would the Department *prefer* that the bill include a statutory provision providing procedures for imposition of capital punishment?

Mr. Cox. The President should have the flexibility to prescribe guidelines and procedures that meet the needs of the armed forces. We would prefer that the statute not constrain his authority in that regard.

Senator Wilson. Mr. Cox, I have a couple of technical questions for you about proposed Article 106A which you did not cover in your statement.

First, I recognize that proposed Article 106A is drafted consistent with the language of existing section 794 of title 18, which is the enforcement responsibility of the Department of Justice. However, it appears that an offense could be committed under that article if a person subject to the Code were to transmit national defense information, whether classified or not, to Great Britain believing that information would be to the advantage of West Germany and without intent or reason to believe it would be harmful to the United States.

How have the courts interpreted section 794 of title 18 with respect to the need for some sort of bad faith on the individual's part, and would the Department limit its use of proposed article 106A to the types of cases to which section 794 has historically been applied?

Mr. Cox. The Supreme Court, in *United States* v. *Gorin*, 412 U.S. 19 (1941) noted that the accused had to be acting in bad faith, and also noted that the phrase regarding information that would be "to the advantage of a foreign country" makes no distinction between friend or enemy because the status of relationships may change.

By incorporating the substantive provisions of section 794, we recognize that the applicable civilian precedents—both from past and those that may be developed in the future—will be given appropriate recognition by the military judiciary and the Court of Military Appeals.

Senator Wilson. Second, recognizing that two distinct foreign countries could be involved in a violation of Article 106A, that is, one country which receives the information and one which is advantaged by its transmission, which of those foreign countries would have to be the Soviet Union or a Communist Nation in order to trigger the mandatory death or life imprisonment clause of the proposed article.

Mr. Cox. The proposed language of S. 1301, like the current statute, proscribes transfer of defense information "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation"; the transfer must be "either directly or indirectly" to a "foreign government" or faction. S. 1301 then differs from current law by providing for death or mandatory life imprisonment "if the foreign government is the Government of the Soviet Union" or any other communist government designated by the President.

As suggested by your question, it is not clear whether the mandatory punishment provisions in S. 1301 refer to the intent clause (that is, the country that is advantaged by the transfer of information) or to the clause referring to the country that receives the information—which may be different from the country that is advantaged.

Senator Wilson. Finally, the mandatory death or life imprisonment clause of proposed Article 106A refers to a Government of the Soviet Union or of any other Communist country. The language appearing earlier in Article 106A refers to advantaging a foreign nation by transmitting information to any foreign Government, faction, party, military or naval force, or to any representative, officer, agent, employee, subject, or citizen thereof.

How would the Department interpret the term Government in the mandatory sentence clause? Would the mandatory sentence phrase be triggered only if the information were transmitted directly to the Government of the Soviet Union or another Communist country?

Mr. Cox. The statute proscribes indirect as well as direct transfers. The difficulty in such circumstances would be in proving that a information transferred to a noncommunist country was intended to be transferred to the Soviet Union. We would prefer deletion of the mandatory sentencing clause. If retained, the language should be clarified to set forth the circumstances in which it would be applicable.

QUESTIONS SUBMITTED BY SENATOR SAM NUNN

Senator NUNN. S. 1301 mandates the death penalty for certain espionage cases. There are currently a number of federal statutes which may be punishable by the death penalty, including the espionage statute. In 1972 the United States Supreme Court in, 408 U.S. 238, struck down the death penalty as unconstitutional absent certain procedural requirements, which have since been specified in various Supreme Court decisions. Although many states have revised their death penalty statutes to meet the requirements set down by the Court, the federal death penalty statutes have not been amended to meet those constitutional standards. There have been several bills introduced, including one in this Congress, which attempt to do that, but none has passed. As I read it, S. 1301 makes no attempt to satisfy the Court, either in amending the UCMJ or Title 18. Wouldn't the death penalty as imposed by this bill be held unconstitutional under the Supreme Court's standards?

Mr. COX. In *United States v. Matthews*, 16 M.J. 354 (C.M.A. 1983), the Court of Military Appeals stated that appropriate procedures for adjudication of the death penalty could be prescribed either by the President or Congress. The President subsequently amended the Manual for Courts-Martial to establish such procedures. The Manual for Courts-Martial would be available to provide constitutionally sufficient death penalty procedures for a new espionage statute under the UCMJ.

The constitutionality of the title 18 amendments made by S. 1301 will be addressed by the Department of Justice in a separate submission to this subcommittee.

Senator NUNN. Since the *Furman* case, the death penalty has been imposed only in homicide cases. In *Coker* v. *Georgia*, 433 U.S. 584 (1971) the Supreme Court found the death penalty impermissible as cruel and unusual punishment for a non-homicidal rape, noting that the rapist "does not take human life" (*Coker, supra* at 598). In his dissent, Chief Justice Burger stated:

The clear implication of today's holding appears to be that the death penalty may be properly imposed only as to crimes resulting in the death of a victim. This casts serious doubt upon the constitutional validity of statutes imposing the death penalty for a variety of conduct which, though dangerous, may not necessarily result in any immediate death, e.g., *treason*, airplane hijacking, and kidnapping. (*Id.*, at 621 (emphasis added).)

In your view, does current federal case law sanction the use of the death penalty for a non-homicidal act such as espionage, regardless of whether the individual is prosecuted under the UCMJ or Title 18?

Mr. COX. Yes. During the last Congress, the Senate approved legislation, S. 1765, which established capital sentencing procedures for espionage and other offenses not involving the death of a victim. I agree with the views of the Senate Judiciary Committee, which noted in its report on S. 1765 that the death penalty for espionage would not be unconstitutional under *Coker*. S. Rep. No. 251, 98th Cong., 1st Sess. 7–8 (1983).

Senator NUNN. In amending the Uniform Code of Military Justice, section 5 of S. 1301 creates a criminal espionage offense punishable by death or life imprisonment which "shall be tried by a general court-martial." Does that language prevent the Justice Department from prosecuting a member of the armed services under the criminal espionage statutes in Title 18?

Mr. COX. No. The quoted phrase refers to the level of trial, not to the choice of forum. It means that a military trial of an offense under Article 106a as proposed in S. 1301 could be held only in a general court-martial, not in a special or summary court-martial. It does not pertain to the relationships between the Departments of Defense and Justice with respect to offenses in which both have jurisdiction.

Senator NUNN. Section 5 of S. 1301 amends the UCMJ by adding a provision entitled "Espionage in Time of Peace." I recognize that the provision is patterned after 18 U.S.C. § 793 and § 794, the civilian espionage statutes, but I am concerned about the breadth of the provision. For example, it is not limited to classified information. It would make it a crime under the UCMJ to pass "any information relating to the national defense" to a foreign nation "with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation."

What is included in the clause "any information relating to the national defense"?

Mr. COX. This phrase is taken directly from the current provisions of 18 U.S.C. § 794 under which both military personnel and civilians may be tried in federal district court may receive a sentence to life imprisonment. Under last year's Senate action, the death penalty also would be authorized. Similar language appears in 18 U.S.C. § 793, which may be incorporated into the military justice system through the third clause of Article 134, 10 U.S.C. § 834.

The Supreme Court, in *United States* v. *Gorin*, 214 U.S. 19, 28 (1941), held that the term "national defense," as used in the statute, "is a generic concept of broad connotations, referring to the military and naval establishments, and the related activities of national preparedness." This is limited by the requirement the action of the accused must be in bad faith and that the information not be of the type that is accessible to the public. *See, e.g., Gorin, supra; United States* v. *Heine*, 141 F.2d 813 (2d Cir. 1945). *cert. denied*, 328 U.S. 833 (1946).

Senator NUNN. What does the clause "to the injury of the United States or to the advantage of a foreign nation" mean?

Mr. COX. These words have been given their ordinary meaning by the courts. These phrases are important in governing the intent requirement, and in providing the basis for concluding that public information is not within the statute. *See Gorin, supra*, at 28.

Senator NUNN. The provision would also apply to a disclosure to a foreign nation, "directly or indirectly." Does this mean that someone who leaks information to the media could be prosecuted under this section?

Mr. COX. To the extent that this question involves an individual who discloses information to the press for the sole purpose of bringing it to the attention of the American public, it is unlikely that such an action would meet the intent requirements of 18 U.S.C. § 794.

Senator NUNN. Do the cases in federal courts interpreting 18 U.S.C. § 793 and § 794 apply to military courts, and if so, would they serve to limit the scope of section 5 of S. 1301?

Mr. COX. When offenses under the Federal Criminal Code are incorporated into the military justice system through the third clause of Article 134, the applicable civilian precedents—and limitations therein—are given appropriate recognition by military courts. Of course, the circumstances involving the standards and responsibilities of members of the armed forces may differ in particular situations from those applicable to their civilian counterparts. Thus, while civilian precedents are taken into account, their specific application in the military setting may take into consideration the unique needs of the armed forces. We would anticipate that the foregoing considerations would be applied by the Court of Military Appeals and the military judiciary in the interpretation of a statute containing substantive provisions identical to 18 U.S.C. § 794.

Senator NUNN. Given the ambiguities in section 5, wouldn't it be preferable to draft a new, carefully drawn provision?

Mr. COX. The espionage statutes were the product of extensive congressional consideration. This legislative history has been influential in litigation regarding these offenses, and the statutes have been limited in scope by the courts. If these settled principles were abandoned in favor of a new statute dealing with the complexities of espionage law, the risk of ambiguity might be considerably increased. So long as section 794 remains in effect in the Federal Criminal Code, its counterpart in the Uniform Code of Military Justice should contain similar substantive provisions.

Senator NUNN. Section 6(a) of S. 1301 is not limited to persons in the Department of Defense. Could it apply to persons in other executive branch agencies? To Congressional staff? To Senators?

Mr. SNIDER. Inasmuch as Section 6(a) specifically indicates that "the Secretary of Defense shall require . . ." the Department would interpret the provision as applying only to those personnel directly under the authority of the Secretary of Defense, i.e., DOD civilian, military and contractor personnel. In this regard, it is noted that DoD is but one of the Executive Branch agencies participating in the SCI program and that the Director of Central Intelligence (DCI) has, under Executive Order 12333, overall responsibility for policy and procedures for determining eligibility of individuals for access to SCI.

Senator NUNN. Subsection 6(b) permits the Secretary of Defense to "require" polygraph examinations to grant access to any classified information. How many persons in the Department of Defense currently have access to classified information? Would it be your proposal to use this authority to polygraph all persons who are cleared for access to classified information?

Mr. SNIDER. There are approximately 4.3 million DoD civilian, military and contractor personnel cleared for access to classified information. Consequently, it would not be possible, given existing resources, to consider polygraph examination of this large number of personnel. The Department believes that requiring counterintelligence-scope polygraph examination for initial access to certain specific categories of extremely sensitive classified information, and selection of individuals who have access to these and other categories of classified information for polygraph examination on an aperiodic, random basis, would establish the polygraph as an effective deterrent to espionage and could be accomplished with a modest expansion of our polygraph examiner training capability.

Senator NUNN. Subsection (e) requires that the polygraph examination be restricted to "relevant issue questions." What do you believe such questions to be? For example, is it relevant to ask an individual whether or not he or she has taken drugs?

Mr. SNIDER. The only relevant questions to be asked during polygraph examinations administered for the purpose of determining eligibility for initial or continued access to classified information are those necessary to determine whether the individual has:

Ever engaged in espionage or sabotage against the United States.

Knowledge of anyone who is engaged in espionage or sabotage against the United States.

Ever been approached to give or sell classified materials to unauthorized persons.

Ever given or sold classified materials to unauthorized persons.

Knowledge of anyone who has given or sold classified materials to unauthorized persons.

Any unauthorized contact with representatives of a foreign government.

Questions concerning use of drugs, credit, sexual behavior, or other "life-style questions would be appropriate only in situations where the individual made admissions which indicated that such matters had had a bearing on involvement in espionage or sabotage, etc. In such cases the polygraph would be utilized to confirm the information provided.

QUESTIONS SUBMITTED BY SENATOR CARL LEVIN

Senator LEVIN. Section 6(c) of the bill states "the results of polygraph examinations shall not be used as the sole basis for denying eligibility for clearance or access to any classified information." Under this provision, could polygraph results be used alone for any purpose? Under Section 6 will polygraph be used for any purpose other than for security clearances?

Mr. SNIDER. To answer this question it is necessary to distinguish between "analysis of polygraph charts," and the "results of a polygraph examination." It has traditionally been the policy of the Department that unfavorable action will not be taken against an individual solely on the basis of the results of an analysis of the polygraph charts. However, the results of the polygraph would encompass any admissions or confessions that the individual might make either before or after collection of the polygraph charts. It is believed that the Department should not be prohibited from using this information in reaching a determination regarding eligibility for access to classified information.

With respect to use of an analysis of polygraph charts, the Department's policy is that when deception is indicated by the examiner's interpretation of polygraph charts, an indepth interview of the subject will be undertaken by the examiner immediately following the running of the charts to resolve such indicated deception. If the indication of deception cannot be resolved through such means, the subject will be so advised and the results of the examination forwarded to the requesting agency. If, after reviewing the polygraph examination results, the requesting agency determines that there is a significant question concerning the subject's clearance or access status, the subject shall be given the opportunity to undergo additional examination using the same or a different examiner. If such additional examination is not sufficient to resolve the matter, a comprehensive investigation of the subject shall be undertaken, using the results of the polygraph examination as an investigative lead. If such investigation develops no derogatory information that could, in and of itself, substantiate taking unfavoirable action, no such unfavorable action shall be permitted.

The only exception to this policy is when the Secretary of Defense, Deputy Secretary of Defense, a Secretary of one of the Military Departments, or the Director of NSA or DIA, determines personally, in writing, that the information in question is of such extreme sensitivity that access under the circumstances poses an unacceptable risk to the national security.

With respect to the second part of the question, the Department believes that it is clear that the legislation applies only to use of the polygraph in connection with determining eligibility for personnel security clearance or access to classified information.

Senator LEVIN. You mentioned in your testimony that an espionage trial which takes place in military court limits public disclosure of classified information. Given this concern with information protection, why do you support reestablishing capital punishment for peacetime espionage under Title 18 of the federal criminal code where the government's interest in limiting public disclosure of classified information conflicts with the extensive rights afforded the accused in a capital case?

Mr. Cox. The rights provided to an accused in a capital case do not create a significantly greater risk of disclosure than the rights applicable in a noncapital case.

Senator LEVIN. Do you think that the provisions in § 1301 establishing capital punishment for peacetime espionage are consistent with the Supreme Court's decision in *Coker* v. *Georgia* which suggests that the death penalty is a disproportionate punishment for non-homicidal offenses? No one has ever been executed for peacetime espionage under Section 794 and the military code of justice has never made peacetime espionage an offense punishable by death. Does this indicate that capital punishment for peacetime espionage may be too severe in relation to the offense?

Mr. Cox. During the last Congress, the Senate approved legislation, S. 1765, which established capital sentencing procedures for espionage and other offenses not involving the death of a victim. I agree with the views of the Senate Judiciary Committee, which noted in its report on S. 1765 that the death penalty for espionage would not be unconstitutional under *Coker.* S. Rep. No. 251, 98th Cong., 1st Sess. 7-8 (1983).

The Department of Justice reports that there have been two executions for espionage under section 794 out of 11 convictions under that statute between 1951 and 1972, the year of the Supreme Court's *Furman.* None of these offenses were directly related to a wartime situation. I do not agree that this indicates that the death penalty may be too severe, particularly in view of the fact that the sentencing process—even before *Furman*—gave great weight to the nature of the offense and offender in each particular case. The absence of a specific capital provision in the UCMJ must be viewed in the context of the availability of the death penalty for servicemembers in federal civilian trials, and does not reflect a legislative judgment exempting servicemembers from this punishment. As to the appropriateness of the death penalty, I concur in the views of the Senate Judiciary Committee report, *supra,* which noted that espionage offenses "are a part of the laws of most countries and commonly, as in current United States law, carry the death penalty as an authorized sentence."

Senator LEVIN. Have there been convictions for espionage under the current provisions in the U.S. Military Code? How many people have been convicted under these statutes? Of those persons convicted under these provisions, how many have been sentenced to death? How many of those sentenced to death have been executed? Please describe the circumstances surrounding those cases in which persons convicted of espionage were sentenced to death and in which the sentences of death were not carried out.

Mr. Cox. Because military justice authority is decentralized, we do not have precise data relating convictions to offenses. Cases in which the sentence, as approved by the convening authority, extended to death, confinement for one year or more, or a punitive discharge, are sent to the Courts of Military Review, and we have somewhat more complete information with respect to reported decisions. Our information with respect to the death penalty is based upon the following review requirements: if the death sentence is approved by the convening authority, there is mandatory review by the Court of Military Review; if the Court of Military Review approves the death sentence, there is mandatory review by the Court of Military Appeals. If the Court of Military Appeals approves the death sentence, it must be acted on by the President before it may be executed. There are few reported cases of espionage-related offenses under the UCMJ and none have involved death as an authorized punishment.

Since the UCMJ became effective in 1951, there have been no convictions for wartime spying under Article 106. None of the convictions for aiding the enemy under Article 104 have been for offenses of the type prosecuted under espionage statutes in the Federal Criminal Code. There has been at least one conviction involving conspiracy and attempt to aid the enemy. The death penalty was not an authorized punishment in that case.

As I noted in my statement, there is no article in the UCMJ that expressly addresses peacetime espionage, and such offenses must be prosecuted in the military justice system under various articles dealing with noncapital offenses. The Courts of Military Review and Court of Military Appeals have affirmed at least six cases under the UCMJ involving offenses related to the Federal Criminal Code's espionage statutes. The death penalty was not an authorized punishment in any of these cases.

Senator LEVIN. You have advocated flexibility in this area in order to achieve specific goals, such as damage limitation. In your testimony you stated: "Frequently in an espionage situation, an investigation may reveal only the tip of the iceberg. There is the need to assess damage, and to probe deeper for other offenders." Once a person has been executed, don't you foreclose all opportunity to "probe deeper"?

Mr. COX. A mandatory death sentence does not preclude all opportunity to "probe deeper." It would remove all incentive for the accused to cooperate fully with counterintelligence authorities. Usually in espionage trials, once counsel for the accused is convinced his client will be convicted, counsel will plea bargain. This could result in a guilty plea in return for only one life sentence versus five life sentences. In return, the prosecution requires a complete statement of all material compromised and the identity and degree of participation of all other persons. This complete statement must be verified by polygraph or the plea bargain is rescinded. A discretionary death penalty would enhance this system which is working well. A mandatory death penalty would harm this important counterintelligence process.

Senator LEVIN. Doesn't the death penalty prevent the Department from negotiating with foreign governments in order to arrange swaps of spies?

Mr. COX. Of course.

Senator WILSON. This hearing is adjourned.

Thank you very much, Mr. Cox.

[Whereupon, at 4:45 p.m., the subcommittee adjourned, subject to the call of the Chair.]

○